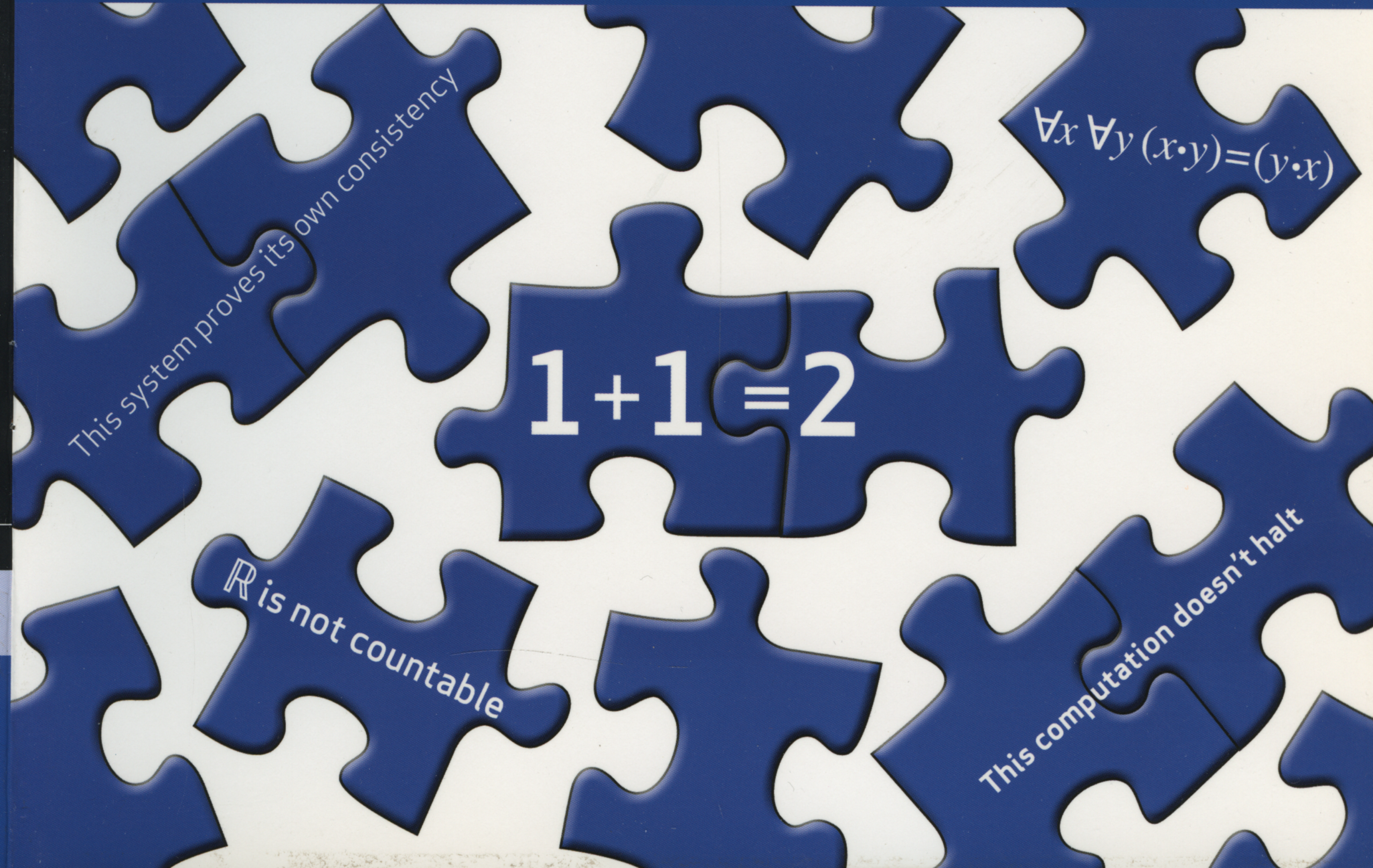
The Open University

M381 Number Theory and
Mathematical Logic

Mathematical Logic **Unit 8**

Gödel's Incompletness Theorems


This system proves its own consistency
∀x ∀y (x•y)=(y•x)
1+1=2
ℝ is not countable
This computation doesn't halt

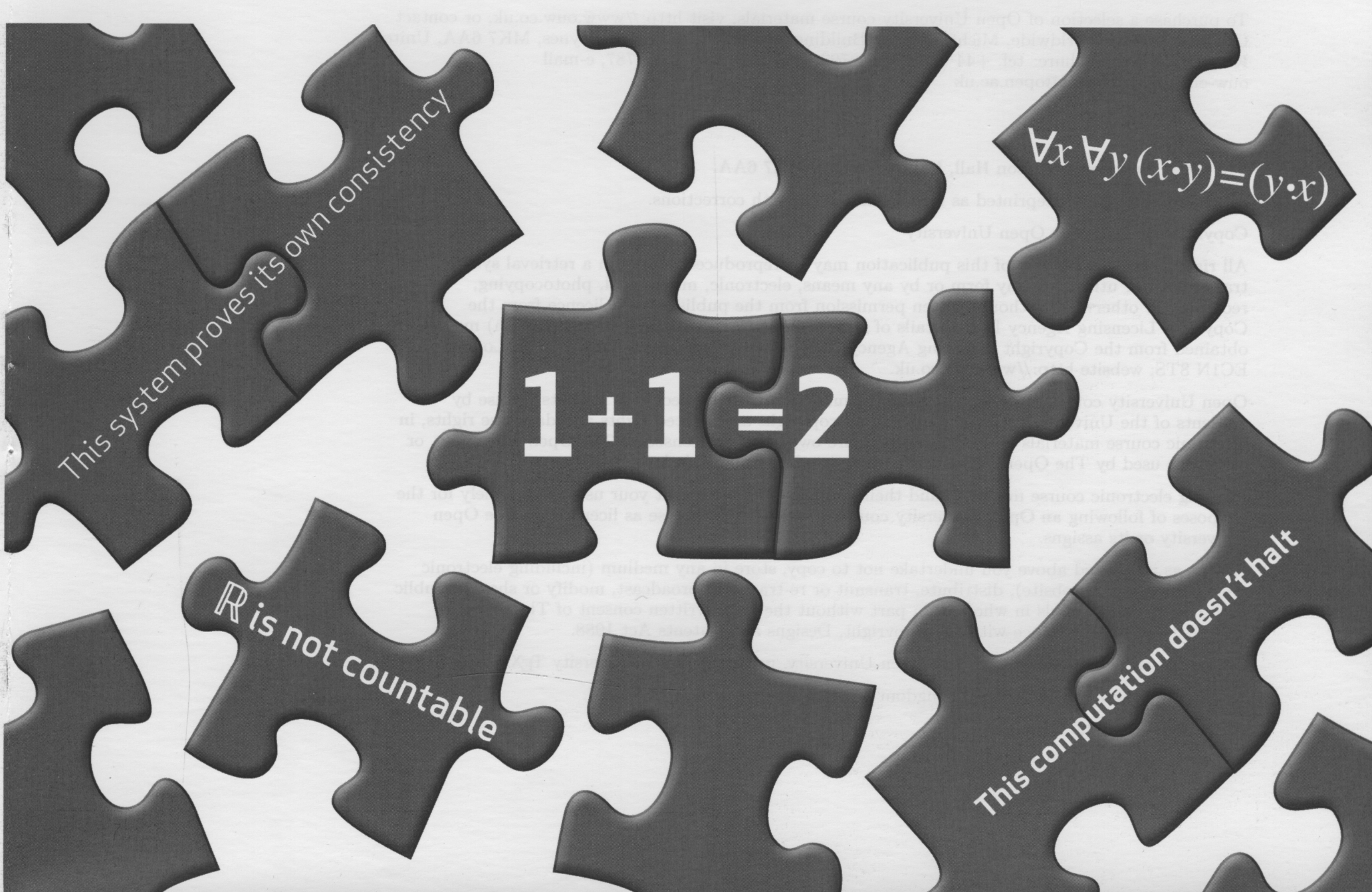
The Open University

M381 Number Theory and
Mathematical Logic

Mathematical Logic Unit 8

Gödel's Incompleteness Theorems

Prepared by the Course Team


This system proves its own consistency
$\forall x \forall y\, (x \cdot y) = (y \cdot x)$
1+1=2
ℝ is not countable
This computation doesn't halt

The M381 Mathematical Logic Course Team

The Mathematical Logic half of the course was produced by the following team:

Roberta Cheriyan	*Course Manager*
Derek Goldrei	*Course Team Chair* and *Academic Editor*
Jeremy Gray	*History Consultant*
Mary Jones	*Critical Reader*
Roger Lowry	*Publishing Editor*
Alan Pears	*Author*
Alan Slomson	*Author*
Frances Williams	*Critical Reader*

with valuable assistance from:

The Maths Production Unit, Learning & Teaching Solutions:
Becky Browne, Jim Campbell, Nicky Kempton, Bill Norman, Sharon Powell, Katie Sayce, Penny Tee

Alison Cadle	*TeX Consultant*
Michael Goldrei	*Cover Design Consultant*
Vicki McCulloch	*Cover Designer*

The external assessor was:

Jeff Paris	*Professor of Pure Mathematics, University of Manchester*

The Course Team would like to acknowledge their reliance on the previous work of Alan Slomson and of Alex Wilkie, Professor of Mathematical Logic, University of Oxford. We would also like to thank the family of Alonzo Church for generously providing the photo of him used in this unit.

This publication forms part of an Open University course. Details of this and other Open University courses can be obtained from the Student Registration and Enquiry Service, The Open University, PO Box 197, Milton Keynes, MK7 6BJ, United Kingdom: tel. +44 (0)870 300 6090, e-mail general-enquiries@open.ac.uk

Alternatively, you may visit the Open University website at http://www.open.ac.uk where you can learn more about the wide range of courses and packs offered at all levels by The Open University.

To purchase a selection of Open University course materials, visit http://www.ouw.co.uk, or contact Open University Worldwide, Michael Young Building, Walton Hall, Milton Keynes, MK7 6AA, United Kingdom, for a brochure: tel. +44 (0)1908 858793, fax +44 (0)1908 858787, e-mail ouw-customer-services@open.ac.uk

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 2004. Reprinted as new edition 2007, with corrections.

Copyright © 2004 The Open University

All rights reserved; no part of this publication may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the publisher or a licence from the Copyright Licensing Agency Ltd. Details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Ltd, Saffron House, 6–10 Kirby Street, London EC1N 8TS; website http://www.cla.co.uk.

Open University course materials may also be made available in electronic formats for use by students of the University. All rights, including copyright and related rights and database rights, in electronic course materials and their contents are owned by or licensed to The Open University, or otherwise used by The Open University as permitted by applicable law.

In using electronic course materials and their contents you agree that your use will be solely for the purposes of following an Open University course of study or otherwise as licensed by The Open University or its assigns.

Except as permitted above you undertake not to copy, store in any medium (including electronic storage or use in a website), distribute, transmit or re-transmit, broadcast, modify or show in public such electronic materials in whole or in part without the prior written consent of The Open University or in accordance with the Copyright, Designs and Patents Act 1988.

Edited, designed and typeset by The Open University, using the Open University TeX System.

Printed and bound in the United Kingdom by Charlesworth Press, Wakefield.

ISBN 978 0 7492 2274 1

3.1

CONTENTS

Introduction 4

1 The Answer to Leibniz's Question 4

1.1 Representability 5

1.2 Algorithmically undecidable theories 8

2 Gödel's First Incompleteness Theorem 10

2.1 Recursively axiomatizable theories 10

2.2 Complete Arithmetic is not recursively axiomatizable 14

3 An Answer to Hilbert's Question 16

3.1 Peano Arithmetic 17

3.2 Gödel's Second Incompleteness Theorem 22

Biographical Sketches 26

Suggestions for Further Reading 30

Summary 33

Objectives 34

Solutions to the Problems 35

Index 40

INTRODUCTION

This final unit brings together all the ideas introduced in the course. These ideas constitute the technical machinery that enables us to prove some very important theorems which answer what we have called Leibniz's and Hilbert's Questions. These theorems, Gödel's Incompleteness Theorems, are among the most profound intellectual discoveries of the twentieth century. Thus you should not be surprised if you find this unit hard going in places. The proofs of almost all the key theorems are given and you should read them to be convinced of their validity. However, our emphasis will be on the *content* of the theorems rather than on the details of their proofs. We hope that, after reading this unit, you will have a good understanding of what these theorems tell us about the scope and limitations of mathematical logic and algorithmic methods.

Section 1 answers Leibniz's Question. Section 2 proves Gödel's First Incompleteness Theorem. Section 3 provides an answer to Hilbert's Question and proves Gödel's Second Incompleteness Theorem. The Biographical Sketches and Suggestions for Further Reading promised in earlier units appear at the end of this unit. There are no Additional Exercises for this unit.

1 THE ANSWER TO LEIBNIZ'S QUESTION

Recall that in *Unit 1* we posed Leibniz's Question in the following way:

> Is there an algorithm for deciding which statements of number theory are true?

In *Unit 4* we introduced a formal language and its standard interpretation $\mathscr{N}$, which enabled us to reformulate Leibniz's Question as:

> Is there an algorithm for deciding which formulas of our formal language are true under the standard interpretation $\mathscr{N}$?

In *Unit 6* we introduced Complete Arithmetic (CA) as the set of sentences of this language which are true in $\mathscr{N}$, and so were able to restate Leibniz's Question as:

> Is there an algorithm for deciding which sentences of our formal language are in the set CA?

In *Unit 1* we saw that the intuitive idea of an algorithm can be replaced by the idea of a URM computation, and in *Unit 3* we saw that the set of URM-computable functions is the same as the set of recursive functions. In order to reformulate Leibniz's Question in terms of recursive functions, which are functions of k-tuples of natural numbers, rather than in terms of formulas of our formal language, we saw in *Unit 4* how we can code these formulas using natural numbers called the Gödel numbers of the formulas. Then, making use of the idea of a recursive set rather than a recursive function, we were able in *Unit 4* to reformulate Leibniz's Question as:

> Is the set of Gödel numbers of those formulas which are true in the standard interpretation $\mathscr{N}$ a recursive set?

Recall from *Unit 2* that a set of numbers A is said to be recursive if its characteristic function χ_A is recursive, where χ_A is defined by

$$\chi_A(n) = \begin{cases} 1, & \text{if } n \in A, \\ 0, & \text{if } n \notin A. \end{cases}$$

Combining this with the definition of CA, we can now restate Leibniz's Question as:

> Is the set of Gödel numbers of the sentences in CA recursive?

It is this question that we can now answer in this section.

1.1 Representability

As we have said, Gödel numbers enable us to apply ideas about recursive sets to sets of formulas. However, as we saw in *Unit 7*, they have a much more subtle use. We can interpret formulas of our formal language as expressing properties of numbers; and, since we have assigned a unique Gödel number to each formula, we can therefore interpret formulas as expressing properties of formulas. This opens the possibility of finding formulas which refer to themselves, and Gödel's Diagonal Lemma shows that this possibility is realized for every theory which extends Q. As we shall shortly see, it is this which enables us, in Subsection 1.2, to give a negative answer to Leibniz's Question.

Theorem 3.5 of *Unit 7*.

To this end, we need some preliminary results about *representable sets*. We prove these in this subsection.

Definition 1.1

A set A is said to be *representable* in a theory T if its characteristic function is representable in T.

The Representability Theorem tells us that total recursive functions are representable in each theory T which extends Q. There is an equivalent result for recursive sets.

Theorem 2.5 of *Unit 7*.

Theorem 1.1

Let T be a theory which extends Q. Then every recursive set is representable in T.

Proof

If A is a recursive set, its characteristic function χ_A is recursive as well as total. Therefore, by the Representability Theorem, χ_A is representable in T, and so A is representable in T. ■

If A is a recursive set, Theorem 1.1 tells us that there is a formula ϕ_A which represents its characteristic function χ_A in the theory T. The next result tells us that we can use such a formula ϕ_A to construct another formula which defines the elements of A in a more direct way.

Theorem 1.2

Let T be a theory which extends Q and let A be a set of natural numbers which is representable in T. Then there is a formula δ_A, in which x is the only variable which may occur freely, such that, for each natural number n:

(a) if $n \in A$ then $\vdash_T \delta_A(\mathbf{n})$;

(b) if $n \notin A$ then $\vdash_T \neg\delta_A(\mathbf{n})$.

Recall that $\mathbf{n}$ is the term consisting of the symbol $\mathbf{0}$ followed by n occurrences of $'$.

Proof

Suppose that ϕ_A is a formula which represents the characteristic function χ_A of A in the theory T. Hence, for all natural numbers n and k, if $\chi_A(n) = k$ then, by the definition of representability:

As χ_A is a characteristic function, the only significant values of k are 0 and 1.

(i) $\vdash_T \phi_A(\mathbf{n}, \mathbf{k})$

(ii) $\vdash_T \forall y\,(\phi_A(\mathbf{n}, y) \rightarrow y = \mathbf{k})$

We let δ_A be the formula $\phi_A(x, \mathbf{1})$. We show that this formula satisfies conditions (a) and (b) of the theorem.

Suppose, first, that $n \in A$. Then $\chi_A(n) = 1$ and hence, by (i), $\vdash_T \phi_A(\mathbf{n}, \mathbf{1})$, that is, $\vdash_T \delta_A(\mathbf{n})$. So condition (a) holds.

Suppose, second, that $n \notin A$. Then $\chi_A(n) = 0$ and hence, by (ii),

$$\vdash_T \forall y\,(\phi_A(\mathbf{n}, y) \rightarrow y = \mathbf{0})$$

Since T extends Q, it follows from Theorem 2.1 of *Unit 7* that

$$\vdash_T \neg\,\mathbf{1} = \mathbf{0}.$$

Now consider the following formal proof.

1	(1)	$\forall y\,(\phi_A(\mathbf{n}, y) \rightarrow y = \mathbf{0})$	Ass
2	(2)	$\neg\,\mathbf{1} = \mathbf{0}$	Ass
3	(3)	$\phi_A(\mathbf{n}, \mathbf{1})$	Ass
1	(4)	$(\phi_A(\mathbf{n}, \mathbf{1}) \rightarrow \mathbf{1} = \mathbf{0})$	UE, 1
1, 3	(5)	$\mathbf{1} = \mathbf{0}$	Taut, 3, 4
1, 2, 3	(6)	$(\mathbf{1} = \mathbf{0}\ \&\ \neg\,\mathbf{1} = \mathbf{0})$	Taut, 2, 5
1, 2	(7)	$(\phi_A(\mathbf{n}, \mathbf{1}) \rightarrow (\mathbf{1} = \mathbf{0}\ \&\ \neg\,\mathbf{1} = \mathbf{0}))$	CP, 6
1, 2	(8)	$\neg\phi_A(\mathbf{n}, \mathbf{1})$	Taut, 7

It follows that

$$\forall y\,(\phi_A(\mathbf{n}, y) \rightarrow y = \mathbf{0}),\ \neg\,\mathbf{1} = \mathbf{0} \vdash \neg\phi_A(\mathbf{n}, \mathbf{1})$$

Hence, as the formulas $\forall y\,(\phi_A(\mathbf{n}, y) \rightarrow y = \mathbf{0})$ and $\neg\,\mathbf{1} = \mathbf{0}$ are derivable in T, so also is the formula $\neg\phi_A(\mathbf{n}, \mathbf{1})$. That is $\vdash_T \neg\delta_A(\mathbf{n})$. So condition (b) also holds. ■

It turns out that the converse of this theorem also holds. We do not use the converse in this unit, but if you want practice in finding formal proofs, you may wish to tackle the following problem which asks you to establish it.

Problem 1.1

Let T be a theory which extends Q and let A be a set of natural numbers such that there is a formula δ_A, with x as its only free variable, for which conditions (a) and (b) of Theorem 1.2 hold. Deduce that the set A is representable in T. *Hint:* Show that, given the assumptions of this problem, the characteristic function of the set A is represented by the formula $((\delta_A(x)\ \&\ y = \mathbf{1}) \vee (\neg\delta_A(x)\ \&\ y = \mathbf{0}))$.

Theorem 1.2 together with the result of Problem 1.1 show that, for a theory T which extends Q, the following conditions on a set A of natural numbers are equivalent.

(a) The set A is representable in T.

(b) There is a formula δ_A whose only free variable is x such that, for each natural number n, if $n \in A$ then $\vdash_T \delta_A(\mathbf{n})$ and if $n \notin A$ then $\vdash_T \neg\delta_A(\mathbf{n})$.

Recall that, in *Unit 6*, we defined a theory T to be *consistent* if there is no sentence Φ such that both $\vdash_T \Phi$ and $\vdash_T \neg\Phi$. We saw that if a theory is *not* consistent then every sentence is derivable in that theory. So an inconsistent theory is of no interest. Thus in subsequent results we build in the assumption that we are dealing with a consistent theory.

Problem 3.2 of *Unit 6*.

We are now ready to prove a key result. It is our first application of Gödel's Diagonal Lemma. We shall see that it has many important consequences.

Theorem 1.3

Let T be a consistent theory which extends Q. Then the set $GN(T)$ of Gödel numbers of the theorems of T is not representable in T.

Proof

Let T be a consistent theory which extends Q. We are aiming to show that there is no formula which represents the set $GN(T)$ of Gödel numbers of the theorems of T within T. We show that no such formula exists by demonstrating that the assumption that such a formula exists leads to a contradiction.

So let us assume that $GN(T)$ is representable in T. Then, by Theorem 1.2, there is a formula θ_T whose only free variable is x such that, for each natural number n,

$$\left.\begin{array}{lcl} n \in GN(T) & \Longrightarrow & \vdash_T \theta_T(\mathbf{n}), \\ n \notin GN(T) & \Longrightarrow & \vdash_T \neg\theta_T(\mathbf{n}). \end{array}\right\} \tag{1.1}$$

Now, as $GN(T)$ is the set of the Gödel numbers of the theorems of T, we have that, for each formula ϕ,

$$\left.\begin{array}{lcl} \vdash_T \phi & \Longrightarrow & \gamma(\phi) \in GN(T), \\ \text{not } \vdash_T \phi & \Longrightarrow & \gamma(\phi) \notin GN(T). \end{array}\right\} \tag{1.2}$$

Recall that $\gamma(\phi)$ is the Gödel number of ϕ and that $\ulcorner\phi\urcorner$ is the term consisting of of the symbol $\mathbf{0}$ followed by $\gamma(\phi)$ occurrences of $'$. In the standard interpretation $\mathscr{N}$ this term is taken as referring to the number $\gamma(\phi)$.

By (1.1) and (1.2), we have

$$\left.\begin{array}{lcl} \vdash_T \phi & \Longrightarrow & \vdash_T \theta_T(\ulcorner\phi\urcorner), \\ \text{not } \vdash_T \phi & \Longrightarrow & \vdash_T \neg\theta_T(\ulcorner\phi\urcorner). \end{array}\right\} \tag{1.3}$$

We now apply Gödel's Diagonal Lemma to the formula $\neg\theta_T$. This tells us that there is a sentence $G_{\neg\theta_T}$ such that

$$\vdash_T (G_{\neg\theta_T} \leftrightarrow \neg\theta_T(\ulcorner G_{\neg\theta_T}\urcorner)) \tag{1.4}$$

To simplify the notation, we shall write G instead of $G_{\neg\theta_T}$, so that (1.4) can be rewritten as

$$\vdash_T (G \leftrightarrow \neg\theta_T(\ulcorner G\urcorner)) \tag{1.5}$$

We now ask whether the sentence G is a theorem of T.

Suppose first that

$$\vdash_T G \tag{1.6}$$

Then, by (1.3),

$$\vdash_T \theta_T(\ulcorner G\urcorner) \tag{1.7}$$

But then, by an application of the Tautology Rule to (1.5) and (1.7), we deduce that

$$\vdash_T \neg G \tag{1.8}$$

Now (1.6) and (1.8) contradict our assumption that T is consistent. Thus supposition (1.6) is wrong, and so we have shown that

$$\text{not } \vdash_T G \tag{1.9}$$

However, now it follows from (1.3) that

$$\vdash_T \neg\theta_T(\ulcorner G\urcorner) \tag{1.10}$$

and, by an application of the Tautology Rule to (1.5) and (1.10), we deduce that

$$\vdash_T G \tag{1.11}$$

But this contradicts (1.9). We have been led to this contradiction because we made the assumption that $GN(T)$ is representable in T. This assumption must therefore be wrong. Thus we have proved that $GN(T)$ is not representable in T. ■

The power of this theorem will become evident from the consequences that we draw from it in the following pages.

Problem 1.2

In the proof of Theorem 1.3 we made two applications of the Tautology Rule. Specify the two tautologies which justify these applications, and check that they are tautologies.

1.2 Algorithmically undecidable theories

We are now able to give an answer to Leibniz's Question. Recall that in the introduction to this section we reformulated this question as:

> Is the set of Gödel numbers of the sentences in CA recursive?

Complete Arithmetic, CA, is a consistent theory which extends Q. Hence, by Theorem 1.1, every recursive set is representable in CA and, by Theorem 1.3, the set $GN(\text{CA})$ is not representable in CA. We can immediately deduce that $GN(\text{CA})$ is not a recursive set. If a sentence is a theorem of CA, it is true in the standard interpretation $\mathcal{N}$ and hence is in CA. Thus $GN(\text{CA})$ is in fact the set of Gödel numbers of all the sentences in CA. Thus we have obtained a negative answer to Leibniz's Question. For the record we formulate this answer as a theorem.

Theorem 1.4 Negative Answer to Leibniz's Question

The set of Gödel numbers of the sentences which are true in the standard interpretation $\mathcal{N}$ is not recursive.

The great interest and importance of this result springs from our work in *Units 1* to *3*, where we showed the connection between recursive functions and computable functions and where we gave evidence for Church's Thesis, which identifies the notions of an algorithmically computable function and of a recursive function. Note also that sentences which we have described as being true 'in the standard interpretation' would more commonly simply be described as being true. Thus we are able to restate Theorem 1.4 in a perhaps more dramatic way which makes clearer its relationship to Leibniz's Question.

Theorem 1.4 Negative Answer to Leibniz's Question (Restated)

There is no algorithm for deciding which statements of number theory are true.

In one sense, this answer to Leibniz's Question is disappointing. If an algorithm for deciding which statements of number theory are true existed, this would enable us to settle all the outstanding questions of number theory in a routine way. On the other hand, it is comforting to know that human ingenuity will always be needed, and that mathematicians cannot be replaced by computers!

Although it may not come as a surprise that there is no algorithm for deciding which sentences are theorems of Complete Arithmetic, it is important to note that the argument used to derive Theorem 1.4 applies also to much weaker theories. Our proof of Theorem 1.4 relies only on Theorems 1.1 and 1.3. Thus it can be generalized immediately to cover any consistent theory which extends Q.

Theorem 1.5

Let T be a consistent theory which extends Q. Then the set of Gödel numbers of the sentences which are theorems of T is not recursive.

In particular, this result applies to the theory Q itself.

Theorem 1.6

There is no algorithm for deciding which sentences are theorems of Q.

This is, in some ways, a more surprising result than Theorem 1.4 because, as we have seen, Q is such a weak theory. We discovered in *Unit 6* that from the axioms of Q we cannot derive, for example, the sentence $\forall x \forall y\,(x+y)=(y+x)$ which expresses the fact that addition of natural numbers is commutative. We gave several more examples of simple facts that cannot be derived from the axioms of Q, showing that it is a weak theory. None the less, Theorem 1.6 shows that the set of theorems of Q is sufficiently complicated that it (or, more strictly, the set of the Gödel numbers of the theorems of Q) is a non-recursive set.

It is even more significant that Q has only a finite number of axioms, indeed just seven. This enables us to deduce from Theorem 1.6 a significant result about quantifier logic, which we anticipated at the end of Subsection 1.2 of *Unit 5*. This result is Church's Theorem, which we shall prove shortly, after proving a couple of preliminary results.

Theorem 1.7

There is no algorithm for deciding, in general, given formulas $\phi_1, \phi_2, \ldots, \phi_k$ and ψ, whether $\phi_1, \phi_2, \ldots, \phi_k \vdash \psi$.

Proof

Let $\sigma_1, \sigma_2, \ldots, \sigma_7$ be the seven sentences which make up the axioms of Q. By Theorem 1.6 there is no algorithm for deciding, given a sentence σ, whether $\vdash_Q \sigma$, that is whether $\sigma_1, \sigma_2, \ldots, \sigma_7 \vdash \sigma$. Hence there cannot be an algorithm for deciding, in general, whether $\phi_1, \phi_2, \ldots, \phi_k \vdash \psi$. ■

Theorem 1.8

There is no algorithm for deciding, in general, given a formula ψ, whether $\vdash \psi$.

Proof

Since $\phi_1, \phi_2, \ldots, \phi_k \vdash \psi$ if and only if $\vdash ((\cdots(\phi_1 \,\&\, \phi_2) \,\&\, \cdots \,\&\, \phi_k) \rightarrow \psi)$, an algorithm for deciding whether a given formula can be derived from no assumptions would enable us to decide, given formulas $\phi_1, \phi_2, \ldots, \phi_k$ and ψ, whether $\phi_1, \phi_2, \ldots, \phi_k \vdash \psi$, contradicting Theorem 1.7. ■

Now sentences which are derivable from no assumptions are, by the Correctness and Adequacy Theorems of *Unit 6*, precisely those sentences which are logically valid, that is, true in all possible interpretations. Thus, from Theorem 1.8, we can deduce the following result.

Theorem 1.9 Church's Theorem

There is no algorithm for deciding which sentences of quantifier logic are logically valid.

This theorem was first proved by Alonzo Church in 1936. It is often paraphrased as 'quantifier logic is algorithmically undecidable'.

We explained in *Unit 5*, at the end of Subsection 1.2, why we could not simply use a 'logical consequence' rule for quantifier logic analogous to the Tautology Rule for propositional logic. We have now proved the theorems which justify our remarks that such a 'logical consequence' rule would fail to have the algorithmic character that we require for a formal system.

2 GÖDEL'S FIRST INCOMPLETENESS THEOREM

In this section we shall look at axioms for number theory within our formal system. In Subsection 3.2 of *Unit 6* we gave some criteria for a set S of axioms for number theory. These included the following.

- There should be an algorithm to determine whether a given sentence is in S.

The other criteria were that all the axioms in S should be true in the standard interpretation $\mathscr{N}$, that we should be able to derive as many theorems as possible from the axioms and that the set of axioms should be as simple as possible.

When we first talked about mathematical proof in *Unit 5* we said that one requirement of a formal system — the machine-checkability requirement — is that there should be an algorithm to decide whether a sequence of formulas satisfies the requirement of being a formal proof. The rules of proof that we introduced in *Units 5* and *6* all meet this requirement. But if we want there to be an algorithm to decide whether a sequence of formulas is a formal proof *from a given set of axioms*, then we also require that there should be an algorithm to decide whether or not a formula is an axiom; hence the above criterion.

The results of the previous section, in particular Theorem 1.4, tell us that the set CA, the set of all sentences of the formal language true in the standard interpretation $\mathscr{N}$, does not meet this criterion. However, this still leaves open the question of whether there is some set S of axioms for CA which does meet the criteria. This is the issue which we look at in this section, culminating in Gödel's First Incompleteness Theorem which resolves it. The criterion that there should be an algorithm to determine whether a given sentence is in the set of axioms is investigated in Subsection 2.1 and the application of this idea to number theory is discussed in Subsection 2.2.

2.1 Recursively axiomatizable theories

In this subsection we look at theories with a set S of axioms for which there is an algorithm to determine whether a given sentence is in S. We make this more precise with the following definition.

Definition 2.1 Recursive axiomatizability

A theory T is said to be *recursively axiomatizable* if it has a set S of axioms whose Gödel numbers form a recursive set.

We shall often refer to a set of axioms whose Gödel numbers form a recursive set as a *recursive set of axioms.* Thus we can say that a theory is recursively axiomatizable if it has a recursive set of axioms. We shall also refer to a set of theorems whose Gödel numbers form a recursive set as a *recursive set of theorems.*

In framing Definition 2.1 we are making a subtle distinction between a theory which has a recursive set of *axioms* and a theory which has a recursive set of *theorems.* The example given by the theory Q shows us that these are not the same thing. The set of axioms of Q is finite and hence is recursive, but Theorem 1.6 tells us that the set of theorems of Q is not recursive. Another example of this kind is given by Theorem 1.8. Thus, despite the negative answer to Leibniz's Question given by Theorem 1.4, there remains the possibility that CA has a recursive set of axioms.

To investigate whether or not such a recursive set of axioms for CA exists, we begin by looking generally in this subsection at properties of theories with a recursive set of axioms or, more precisely, at the corresponding sets of Gödel numbers of theorems. First we introduce a new way of describing sets of natural numbers.

Definition 2.2 Recursive enumerability

A set X of natural numbers is said to be *recursively enumerable* if either X is empty or X can be expressed in the form

$$X = \{f(0), f(1), f(2), \ldots\}$$

where f is a total recursive function.

In other words, a non-empty set of natural numbers is recursively enumerable if it is the set of values taken by a total recursive function. Note that our notation is not intended to imply that the values $f(0), f(1), f(2), \ldots$ are all distinct. Thus, as shown by Example 2.1 below, a recursively enumerable set can be finite, while Example 2.3 provides an instance of an infinite set enumerated by a recursive function whose values are not all distinct. It is convenient to regard the empty set as being recursively enumerable, and, as this set cannot be the set of values taken by a total function, in our definition we need to specify separately that the empty set is recursively enumerable.

By Church's Thesis, a function f is recursive if and only if there is an algorithm for computing its values. So a set is recursively enumerable if and only if either it is empty or there is an algorithm for enumerating (or listing) its members.

There is an important, but quite subtle, difference between a recursive set and a recursively enumerable set, as we shall see later.

Example 2.1

The set $\{0\}$ is recursively enumerable. The zero function $\text{zero}: n \longmapsto 0$ is recursive and the set of values taken by this function is just the set $\{0, 0, 0, \ldots\} = \{0\}$.

◆

Example 2.2

The set $\{0, 1, 4, 9, \ldots\}$ of squares is recursively enumerable. The function $f: n \longmapsto n^2$ is recursive and the set of squares is the set of values taken by this function.

◆

Example 2.3

The set Y of all natural numbers whose decimal representations occur as consecutive digits somewhere to the right of the decimal point in the infinite decimal expansion of π is a recursively enumerable set.

We demonstrate this by means of an informal argument. As

$$\pi = 3.14159\ldots$$

the set Y includes, for example, 5 (coming from the underlined part of $3.141\underline{5}9\ldots$), 415 (coming from $3.1\underline{415}9\ldots$) and so on.

There are well-known algorithms, based for example on convergent series, that enable us to compute the decimal expansion of π to as many places as we wish. We can use such an algorithm to enumerate all finite strings of digits which occur after the decimal point as follows:

Step 1 Generate the first digit after the decimal point: $\pi = 3.1\ldots$ so the list begins $\{1, \ldots\}$.

Step 2 Generate the next digit: $\pi = 3.14\ldots$ so we add to the list 4 and 14 giving $\{1, 4, 14, \ldots\}$.

Step 3 Generate the next digit: $\pi = 3.141\ldots$ so we add to the list 1, 41 and 141 giving $\{1, 4, 14, 41, 141, \ldots\}$.

⋮

It doesn't matter that the string 1 gets repeated by this process, here at *Step 3*. The values of the enumerating function need not be distinct.

Given an algorithm for generating the decimal expansion of π as far as we like, we have an algorithm which enables us to continue the list as far as we like. Thus if f is defined by $f(n) =$ the nth number in the list (counting 1 as $f(0)$), we see that Y is the set of values taken by a total computable function f and hence Y is recursively enumerable. ◆

Our argument in Example 2.3 is an example of the use of Church's Thesis. We have relied on the fact that we can describe informally an algorithm for computing the values of f to deduce that f is a recursive function. In this way we have avoided the technical complexities of a more precise proof that f is a recursive function. In what follows we shall continue to use informal arguments of this kind.

Problem 2.1

Show that the set $\{2, 3, 8\}$ is recursively enumerable.

Problem 2.2

Show that every finite set of natural numbers is recursively enumerable.

Problem 2.3

Show that every recursive set of natural numbers is recursively enumerable. *Hint:* If A is a recursive set of natural numbers, its characteristic function χ_A is a total recursive function. Use χ_A to devise a total recursive function whose set of values is precisely the set A.

From our point of view the most important examples of recursively enumerable sets are those given by the next theorem. Before coming to this, we need to remind ourselves that in *Unit 4*, Subsection 2.2, we showed how to assign Gödel numbers to formulas, and to indicate how we can extend this numbering to formal proofs.

Recall that a formal proof consists of a numbered finite sequence of formulas together with justifications explaining how each formula in the sequence has been obtained using the rules of proof. We already know how to assign a Gödel number $\gamma(\phi)$ to each formula ϕ. This Gödel numbering exploits the fact that the formulas consist of finite sequences of the basic symbols, and that these basic symbols are drawn from a finite list. The justifications, such as Taut, 3, 5 and Ass, that occur in a formal proof also consist of finite

Note that we don't have to concern ourselves with the assumption numbers, given to the left of each line of a proof, as these can be calculated from the justifications.

sequences of symbols drawn from the finite list made up of the letters of the English alphabet, the standard numerals $0, 1, \ldots, 9$ and a comma. Thus, by assigning Gödel numbers to each of these symbols, we can duplicate the technique for assigning Gödel number to formulas to enable us to assign Gödel numbers to justifications. Let us denote the Gödel number assigned to a justification j as $\delta(j)$. Then, for any formal proof F given by

$$\begin{array}{lll} (1) & \phi_1 & j_1 \\ (2) & \phi_2 & j_2 \\ \vdots & & \\ (k) & \phi_k & j_k \end{array}$$

we assign to it the Gödel number

$$\Gamma(F) = 2^{\gamma(\phi_1)} 3^{\delta(j_1)} \ldots p_{2k-1}^{\gamma(\phi_k)} p_{2k}^{\delta(j_k)}$$

where p_i is the ith prime number.

Γ is Greek letter 'capital gamma', corresponding to the lower-case γ. We use the capital letter Γ to distinguish the Gödel number of a proof from the Gödel number $\gamma(\phi)$ of a formula ϕ.

It should now be evident that, if we are given a natural number n, we can first compute whether or not n is the Gödel number of a formal proof, and if it is we can compute from n the Gödel numbers of the formulas which are the assumptions in force on the last line of the proof.

We are now ready to prove the key theorem of this subsection.

Theorem 2.1

The set $GN(T)$ of Gödel numbers of the theorems of a recursively axiomatizable theory T form a recursively enumerable set.

Proof

Let T be a theory with a recursive set S of axioms.

The set of theorems of T is certainly not empty. For example, it includes the sentence

$$\forall x_0\, x_0 = x_0$$

We let n_0 be the Gödel number of this sentence.

An explicit expression for n_0 is given in Subsection 2.2 of *Unit 4*.

We define a recursive function f by giving an informal description of an algorithm for computing the values of f.

Given $n \in \mathbb{N}$, first compute whether n is the Gödel number of a formal proof.

If not we put $f(n) = n_0$.

If n is the Gödel number of a formal proof, we can compute from n the Gödel numbers of the assumptions on which the last line of this proof depends. Then, as S is a recursive set of axioms, we can compute whether or not all these assumptions are in S. If all these assumptions are in S, then we put

$f(n) =$ the Gödel number of the formula on the last line of the proof;

if not, we put $f(n) = n_0$, as before.

Thus, for all $n \in \mathbb{N}$, $f(n)$ is the Gödel number of a formula which can be derived from assumptions which are in S, and hence $f(n)$ is the Gödel number of a theorem of T.

Conversely, if ϕ is a theorem of T, there is a formal proof, say F, of ϕ from assumptions in S. So $\Gamma(F)$ is the Gödel number of such a proof, and hence $f(\Gamma(F)) = \gamma(\phi)$, that is, $f(\Gamma(F))$ is the Gödel number of ϕ.

Thus $\{f(0), f(1), f(2), \ldots\}$ is the set $GN(T)$ of all the Gödel numbers of the theorems of T. Since f is a total recursive function, it follows that this set is recursively enumerable. ■

In giving the proof of Theorem 2.1, we have relied heavily on Church's Thesis. However, note that we have only used it in what we described in *Unit 3* as the practical sense, in which it expresses our confidence that we could turn the informal algorithm for computing the values of f, as described in the proof, into a precise proof that f is a recursive function.

2.2 Complete Arithmetic is not recursively axiomatizable

It follows from Theorem 2.1 that the set $GN(Q)$ of Gödel numbers of the theorems of Q is recursively enumerable. This is in contrast with the result of Theorem 1.6, which tells us that this set is not recursive. Thus $GN(Q)$ provides us with an example of a set which is recursively enumerable but not recursive. This means that, although we can enumerate this set as

$$GN(Q) = \{f(0), f(1), f(2), \ldots\}$$

where f is a recursive function, there is no algorithm for determining whether or not a given number is in this set. The moral to be drawn here is that the existence of an algorithm for *enumerating* the theorems of a recursively axiomatizable theory does not imply the existence of an algorithm for *deciding* whether or not a given sentence is a theorem: 'wait and see if it appears in the list' is not an algorithm for giving an answer to this question. If a sentence is a theorem then it will appear at some stage of the enumeration, and when it does appear we shall know that it is a theorem; but if a sentence is not a theorem, there may never be a stage when we can be sure of this, since the fact that a sentence has not so far appeared in the enumeration may not give us any information about whether it will appear later.

There is, however, one special case where we can deduce that a recursively axiomatizable theory has a recursive set of theorems. Recall that a theory T is said to be *complete* if, for every sentence Φ of the formal language, either $\vdash_T \Phi$ or $\vdash_T \neg\Phi$. We noted in Section 3 of *Unit 6* that if T is the set of all sentences which are true in some particular interpretation of the formal language then T is complete. In particular Complete Arithmetic, which is the set of all sentences true in the standard interpretation, is a complete theory.

Definition 3.4 of *Unit 6*.

Theorem 2.2

A complete recursively axiomatizable theory has a recursive set of theorems.

Proof

Let T be a complete recursively axiomatizable theory.

We note first that, if T is not consistent, then every sentence is a theorem of T and so, in a very uninteresting way, there is an algorithm for deciding which sentences are theorems of T. Thus from now on we need only consider the case where T is a consistent theory.

Problem 3.2 of *Unit 6*.

By Theorem 2.1, there is an algorithm for enumerating the theorems of T. Suppose that this algorithm produces the list

$$\Phi_0, \Phi_1, \Phi_2, \ldots$$

of all the theorems of T. We describe an algorithm for deciding whether or not a given sentence Φ is a theorem of T.

Given a sentence Φ, we know that, as T is complete, either Φ or $\neg\Phi$ is a theorem of T, and that, as T is consistent, they cannot both be theorems of T. Thus after a finite number of steps of the enumeration, one of Φ and $\neg\Phi$ must appear in the list. If it is Φ which appears, then we can deduce that Φ is a theorem of T. If it is $\neg\Phi$ which appears, we can deduce that Φ does not occur anywhere in the list and so is not a theorem of T. So in either case, after a finite number of steps the algorithm terminates with a correct answer as to whether or not Φ is a theorem of T. ■

We now come to the main theorem of the course.

Theorem 2.3 Gödel's First Incompleteness Theorem

There is no complete and consistent recursively axiomatizable extension of Q.

Proof

By Theorem 2.2, if T were a complete and consistent recursively axiomatizable theory which extends Q, then T would have a recursive set of theorems. But this contradicts Theorem 1.5. Hence no such complete and consistent extension of Q exists. ■

Theorem 2.4

Complete Arithmetic is not recursively axiomatizable.

Proof

Since Complete Arithmetic is a complete and consistent extension of Q, it is an immediate consequence of Theorem 2.3 that Complete Arithmetic is not recursively axiomatizable. ■

Theorem 2.3 is known as an 'incompleteness' theorem because it may be reformulated as follows.

> If T is a consistent recursively axiomatizable extension of Q, then T is not complete.

Gödel first announced this theorem publicly at a meeting in Königsberg in September 1930. The details of the proof were given in his paper which was published in the following year. Although the proof we have given here uses essentially the same methods and ideas as Gödel's first published proof, it differs from it in some significant respects.

For bibliographical details, see the Suggestions for Further Reading at the end of this unit.

First, in his 1931 paper Gödel points out that his proof works for any theory sufficiently powerful that every recursive relation is representable in it. However, in 1931 it was not realized that there are systems as weak as the finitely axiomatizable theory Q in which all total recursive functions are representable. Thus Gödel took as his base theory one which is significantly more powerful than Q.

We shall discuss this theory in Section 3.

Second, our proof of Theorem 2.3 depends on deducing it from Theorem 1.5, and hence ultimately from Theorem 1.3. It is in our proof of Theorem 1.3 that we made heavy use of Gödel's ideas and in particular the device of Gödel numbering and Gödel's Diagonal Lemma. In contrast, Gödel gave a direct proof of Theorem 2.3 in which he uses his methods to show how to construct, for a given recursively axiomatized consistent extension T of Q, a sentence σ_T such that neither σ_T nor $\neg\sigma_T$ is a theorem of T. This shows directly that T is not complete. Moreover, it can be seen from the construction of the sentence σ_T that $\neg\sigma_T$ is true in the standard interpretation. Thus Gödel's proof provides an example of a sentence which is true (in the standard interpretation) but which is not a theorem of T.

We say more about this in the next section.

What was missing in 1931 was an appreciation of Theorem 2.2, which for us enables us to deduce Theorem 2.3 very readily from Theorem 1.5. From our viewpoint, with our experience of recursive and recursively enumerable sets, it is rather surprising that the truth of Theorem 2.2, whose proof to us seems very straightforward, was overlooked at the time. Gödel's First Incompleteness Theorem shows that Complete Arithmetic cannot be recursively axiomatized. This result came as a considerable surprise. However, Theorem 2.2 shows that if Complete Arithmetic could be recursively axiomatized, then there would be an algorithm for deciding which sentences of number theory are true in the standard interpretation, a result that even in 1931 might have seemed implausible.

3 AN ANSWER TO HILBERT'S QUESTION

In this section we shall answer Hilbert's Question:

> Can the consistency of number theory be proved using only non-dubious principles of finitary reasoning?

One of our purposes in setting up our formal system in *Units 4* to *6* was to provide a framework for proof based on finitary reasoning. Within this framework, we need to choose a set of axioms for number theory so that we can investigate Hilbert's Question with the corresponding theory. To ensure finitary reasoning, we want a theory with a set of axioms which is at the very least recursive, so that Complete Arithmetic is unsuitable. At the other end of the spectrum, the theory Q is plainly too weak to be considered as number theory for this purpose. In Subsection 3.1 we shall look at the theory *Peano Arithmetic* which provides a useful and important compromise between these unsuitable theories and in Subsection 3.2 we answer Hilbert's Question for this theory.

3.1 Peano Arithmetic

Gödel's First Incompleteness Theorem tells us that no consistent recursively axiomatizable extension of Q is complete. This theorem applies to the theory Q itself. But, of course, it is no surprise that Q is not complete. In Section 3 of *Unit 6* we noted many examples of sentences which are true in the standard interpretation $\mathscr{N}$ but are not theorems of Q. These include such simple sentences as $\forall x \neg x' = x$ and $\forall x \forall y\,(x+y) = (y+x)$. Thus Q is a weak theory. In this subsection we introduce a much more powerful consistent recursively axiomatizable theory whose theorems include many more sentences which are true in the standard interpretation.

The surprising thing about Q is that, despite being a weak theory, its theorems do not form a recursive set.

From your studies in the Number Theory part of M381, you will probably find it easy to see what is missing from Q that makes it such a weak theory. One of the most common methods of proof in number theory is Mathematical Induction, but there is nothing in the theory Q which corresponds to this.

The Principle of Mathematical Induction is formulated in *Unit 1* of Number Theory in the following way.

Principle of Mathematical Induction

Let $P(n)$ be a proposition depending on a natural number n. If:

(a) $P(0)$ is true;

(b) for each natural number k, if $P(k)$ is true then $P(k+1)$ is true;

then $P(n)$ is true for all $n \in \mathbb{N}$.

We have changed the wording slightly from that given in *Unit 1* of Number Theory to allow for the fact that we are dealing with the set of natural numbers, starting at 0, rather than with the positive integers, starting at 1.

The theory we are about to study attempts to incorporate this principle into its axioms. What we need is a formal counterpart to the notion of a 'proposition depending on a natural number n' used to formulate the principle above.

We have seen in *Units 4* and 5 that, if ϕ is a formula in which the variable x occurs freely, then whether or not ϕ is true in the standard interpretation $\mathscr{N}$ depends on how we interpret x, that is, on which natural number we regard x as representing. In this way we can think of ϕ as expressing a proposition which depends on a natural number.

The formula ϕ will be true in the standard interpretation when x is interpreted as the natural number n if and only if $\phi(\mathbf{n}/x)$ is true in this interpretation, where $\phi(\mathbf{n}/x)$ denotes the formula obtained by substituting the term $\mathbf{n}$ for all free occurrences of the variable x in ϕ. To fit in better with the notation used in expressing the Principle of Mathematical Induction, we shall write $\phi(\mathbf{n})$ instead of $\phi(\mathbf{n}/x)$. More generally, we shall write $\phi(\tau)$ instead of $\phi(\tau/x)$. It follows that $\phi(x)$ is the same as the formula ϕ; writing it as $\phi(x)$ emphasizes that we are interested in the fact that the variable x has free occurrences in ϕ, so that ϕ can be interpreted as expressing a property of natural numbers.

The notation $\phi(\mathbf{n}/x)$, or more generally $\phi(\tau/x)$, was introduced in *Unit 5*.

The notation $\phi(\mathbf{n})$ was introduced (albeit in a different context) in *Unit 7*.

Thus we are now able to give a formal counterpart of the Principle of Mathematical Induction, as follows.

Let ϕ be a formula in which the variable x may occur freely. Then the formulas $\phi(\mathbf{0})$, $\forall x\,(\phi(x) \to \phi(x'))$ imply $\forall x\,\phi(x)$.

Here, $\phi(\mathbf{0})$ is the counterpart of '$P(0)$ is true', $\forall x\,(\phi(x) \to \phi(x'))$ corresponds to 'for each natural number k, if $P(k)$ is true then $P(k+1)$ is true' and $\forall x\,\phi(x)$ corresponds to the conclusion '$P(n)$ is true for all $n \in \mathbb{N}$'.

Thus one way to incorporate the Principle of Mathematical Induction into our theory would be to take sentences of the form

$$((\phi(\mathbf{0}) \mathbin{\&} \forall x\,(\phi(x) \rightarrow \phi(x'))) \rightarrow \forall x\,\phi(x))$$

as axioms. In fact, in practice we shall also wish to use such axioms in the cases where the formula ϕ has, in addition, free occurrences of variables other than x. In such cases we need to prefix universal quantifiers for these other variables in order to express the truth of the above formula however these other variables are interpreted. For example, if ϕ is a formula in which x and y, but no other variables, may occur freely, then we need to take the sentence

$$\forall y\,((\phi(\mathbf{0}, y) \mathbin{\&} \forall x\,(\phi(x, y) \rightarrow \phi(x', y))) \rightarrow \forall x\,\phi(x, y))$$

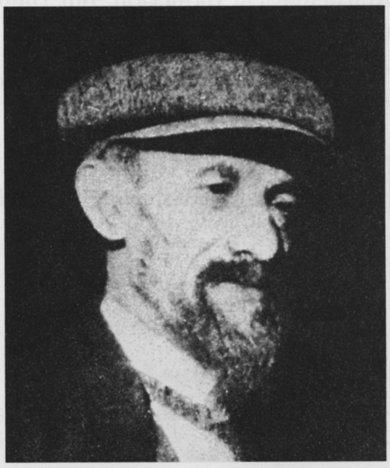
as an axiom. The theory we get by adding to the axioms of Q all sentences of this form is called *Peano Arithmetic* and is denoted by PA.

Definition 3.1 Peano Arithmetic

Peano Arithmetic is the theory PA whose axioms consist of the axioms $Q1$ to $Q7$ of Q together with all sentences of the formal language obtained from formulas of the form

$$((\phi(\mathbf{0}) \mathbin{\&} \forall x\,(\phi(x) \rightarrow \phi(x'))) \rightarrow \forall x\,\phi(x))$$

by prefixing universal quantifiers for all variables which occur freely. Axioms of this latter form are called *induction axioms*.



Giuseppe Peano 1858–1932.

The German mathematician Richard Dedekind (1831–1916) was first to characterize the natural numbers by axioms which included the Principle of Mathematical Induction. The Italian mathematician Giuseppe Peano devised a more formal set of axioms for number theory in 1889 and the theory PA is named after him.

Like the axioms of Q, the induction axioms are all true in the standard interpretation $\mathscr{N}$. Hence all the theorems of PA are true in the standard interpretation and hence PA is a consistent theory. It is evidently an extension of Q. Although there are infinitely many induction axioms, it is not difficult to see that there is an algorithm for determining whether a formula has the form of an induction axiom. Hence the axioms of PA form a recursive set. Thus PA is a consistent recursively axiomatizable extension of Q, and hence, by Theorem 2.3, PA is not complete.

Although incomplete, PA is a very much more powerful theory than Q, because it includes all the induction axioms. The proofs of a great number of the known theorems of number theory can be given in the theory PA. We do not have the time to go very far in exploring the strength of this system. The evidence that had accumulated by 1930 certainly suggested that it might be possible to derive all the true sentences of number theory, that is all the sentences of our formal language which are true in the standard interpretation, in the theory PA. That is why it was a shock when Gödel published the proof of his First Incompleteness Theorem in 1931. Gödel's paper of 1931 was based on a formal system which is essentially the same as PA.

Example 3.1

Our first example of a formal proof using an induction axiom shows that, with its aid, we can derive the axiom $Q3$ from the remaining axioms of PA.

We let $\phi(x)$ be the formula $(\neg\, x = \mathbf{0} \rightarrow \exists y\, x = y')$. Thus $\phi(\mathbf{0})$ is the formula

$$(\neg\, \mathbf{0} = \mathbf{0} \rightarrow \exists y\, \mathbf{0} = y') \tag{3.1}$$

and $(\phi(x) \rightarrow \phi(x'))$ is the formula

$$((\neg\, x = \mathbf{0} \rightarrow \exists y\, x = y') \rightarrow (\neg\, x' = \mathbf{0} \rightarrow \exists y\, x' = y')) \tag{3.2}$$

We show that (3.1) and (3.2) are both theorems of PA, and then, by using the appropriate induction axiom, that $\forall x\, \phi(x)$ is a theorem of PA.

	(1)	$\mathbf{0} = \mathbf{0}$	II
	(2)	$\phi(\mathbf{0})$	Taut, 1
	(3)	$x' = x'$	II
	(4)	$\exists y\, x' = y'$	EI, 3
	(5)	$(\phi(x) \rightarrow \phi(x'))$	Taut, 4
	(6)	$\forall x\, (\phi(x) \rightarrow \phi(x'))$	UI, 5
7	(7)	$((\phi(\mathbf{0})\ \&\ \forall x\, (\phi(x) \rightarrow \phi(x'))) \rightarrow \forall x\, \phi(x))$	Ass
7	(8)	$\forall x\, \phi(x)$	Taut, 2, 6, 7

Note that the assumption on line 7 is an induction axiom. Hence $\vdash_{\mathrm{PA}} \forall x\, \phi(x)$.

Now let PA$'$ be the theory obtained from PA by removing the axiom $Q3$. The formal proof above shows that

$$\vdash_{\mathrm{PA}'} \forall x\, (\neg\, x = \mathbf{0} \rightarrow \exists y\, x = y')$$

That is, axiom $Q3$ is a theorem of PA$'$. Thus the inclusion of $Q3$ in the set of axioms of PA was not necessary.

◆

Example 3.2

We show that

$$\vdash_{\mathrm{PA}} \forall x\, (\mathbf{0} + x) = x$$

We observed in *Unit 6*, Subsection 3.2, that the sentence $\forall x\, (\mathbf{0} + x) = x$ is not a theorem of Q, so this example shows that PA is more powerful than Q.

Let $\phi(x)$ be the formula $(\mathbf{0} + x) = x$. Thus $\phi(\mathbf{0})$ is the formula

$$(\mathbf{0} + \mathbf{0}) = \mathbf{0} \tag{3.3}$$

and $(\phi(x) \rightarrow \phi(x'))$ is the formula

$$((\mathbf{0} + x) = x \rightarrow (\mathbf{0} + x') = x') \tag{3.4}$$

We show that (3.3) and (3.4) are both theorems of PA, and then, by using the appropriate induction axiom, that $\forall x\, \phi(x)$ is a theorem of PA.

1	(1)	$\forall x\, (x + \mathbf{0}) = x$	Ass
2	(2)	$\forall x \forall y\, (x + y') = (x + y)'$	Ass
3	(3)	$\phi(x)$	Ass
1	(4)	$\phi(\mathbf{0})$	UE, 1
2	(5)	$\forall y\, (\mathbf{0} + y') = (\mathbf{0} + y)'$	UE, 2
2	(6)	$(\mathbf{0} + x') = (\mathbf{0} + x)'$	UE, 5
2, 3	(7)	$\phi(x')$	Sub, 3, 6
2	(8)	$(\phi(x) \rightarrow \phi(x'))$	CP, 7
2	(9)	$\forall x\, (\phi(x) \rightarrow \phi(x'))$	UI, 8
10	(10)	$((\phi(\mathbf{0})\ \&\ \forall x\, (\phi(x) \rightarrow \phi(x'))) \rightarrow \forall x\, \phi(x))$	Ass
1, 2, 10	(11)	$\forall x\, \phi(x)$	Taut, 4, 9, 10

Assumptions 1 and 2 are axioms $Q4$ and $Q5$, respectively. Assumption 10 is an induction axiom. Thus all the three assumptions on which the last line depends are axioms of PA. Hence $\vdash_{\mathrm{PA}} \forall x\, \phi(x)$, that is $\vdash_{\mathrm{PA}} \forall x\, (\mathbf{0} + x) = x$.

◆

Problem 3.1

Show that

$$\vdash_{\mathrm{PA}} \forall x\,(\mathbf{0} \cdot x) = \mathbf{0}$$

Problem 3.2

Show that

$$\vdash_{\mathrm{PA}} \forall x\,(x \cdot \mathbf{0}') = x$$

Hint: Show that $\vdash_Q (\forall x\,(\mathbf{0} + x) = x \to \forall x\,(x \cdot \mathbf{0}') = x)$ and then use the result of Example 3.2.

Although the theory PA is very powerful, formal proofs even of quite simple results are rather long. So we shall not try to prove many more results in PA. In fact, we shall simply show that, in the theory PA, we can prove that addition is commutative. We begin with a preliminary result.

Because of the lengths of these proofs, you may decide to take the details on trust.

Example 3.3

We show that

$$\vdash_{\mathrm{PA}} \forall x \forall y\,(y' + x) = (y + x)'$$

Let $\phi(x)$ be the formula $\forall y\,(y' + x) = (y + x)'$. We aim to show that both $\vdash_{\mathrm{PA}} \phi(\mathbf{0})$ and $\vdash_{\mathrm{PA}} \forall x\,(\phi(x) \to \phi(x'))$. Then a routine use of an induction axiom will enable us to deduce that $\vdash_{\mathrm{PA}} \forall x\,\phi(x)$.

Thus we show first that $\vdash_{\mathrm{PA}} \phi(\mathbf{0})$. Consider the following formal proof.

1	(1)	$\forall x\,(x + \mathbf{0}) = x$	Ass
1	(2)	$(y' + \mathbf{0}) = y'$	UE, 1
1	(3)	$(y + \mathbf{0}) = y$	UE, 1
	(4)	$(y + \mathbf{0}) = (y + \mathbf{0})$	II
1	(5)	$y = (y + \mathbf{0})$	Sub, 3, 4
1	(6)	$(y' + \mathbf{0}) = (y + \mathbf{0})'$	Sub, 2, 5
1	(7)	$\forall y\,(y' + \mathbf{0}) = (y + \mathbf{0})'$	UI, 6

The assumption on which the last line of this proof depends is axiom $Q4$. Hence the proof shows that $\vdash_{\mathrm{PA}} \phi(\mathbf{0})$. (In fact it shows that also $\vdash_Q \phi(\mathbf{0})$.)

Now consider the following formal proof.

1	(1)	$\forall x \forall y\,(x + y') = (x + y)'$	Ass
2	(2)	$\phi(x)$	Ass
2	(3)	$(y' + x) = (y + x)'$	UE, 2
1	(4)	$\forall y\,(z + y') = (z + y)'$	UE, 1
1	(5)	$(z + x') = (z + x)'$	UE, 4
1	(6)	$\forall z\,(z + x') = (z + x)'$	UI, 5
1	(7)	$(y' + x') = (y' + x)'$	UE, 6
1, 2	(8)	$(y' + x') = (y + x)''$	Sub, 3, 7
1	(9)	$(y + x') = (y + x)'$	UE, 6
	(10)	$(y + x') = (y + x')$	II
1	(11)	$(y + x)' = (y + x')$	Sub, 9, 10
1, 2	(12)	$(y' + x') = (y + x')'$	Sub, 8, 11
1, 2	(13)	$\phi(x')$	UI, 12
1	(14)	$(\phi(x) \to \phi(x'))$	CP, 13
1	(15)	$\forall x\,(\phi(x) \to \phi(x'))$	UI, 14

The assumption on which the last line of this proof depends is the axiom $Q5$. Hence we can deduce that $\vdash_{\mathrm{PA}} \forall x\,(\phi(x) \to \phi(x'))$. (Again, in fact, we have $\vdash_{Q} \forall x\,(\phi(x) \to \phi(x'))$.)

Since $\vdash_{\mathrm{PA}} \phi(\mathbf{0})$ and $\vdash_{\mathrm{PA}} \forall x\,(\phi(x) \to \phi(x'))$, a straightforward use of the induction axiom $((\phi(\mathbf{0})\ \&\ \forall x\,(\phi(x) \to \phi(x'))) \to \forall x\,\phi(x))$ together with the Tautology Rule enables us to deduce that $\vdash_{\mathrm{PA}} \forall x\,\phi(x)$, that is $\vdash_{\mathrm{PA}} \forall x\,\forall y\,(y' + x) = (y + x)'$.

Example 3.4

We show that

$$\vdash_{\mathrm{PA}} \forall x\,\forall y\,(x + y) = (y + x)$$

Let $\phi(x)$ be the formula $\forall y\,(x + y) = (y + x)$. As in the previous example we aim to prove that both $\vdash_{\mathrm{PA}} \phi(\mathbf{0})$ and $\vdash_{\mathrm{PA}} \forall x\,(\phi(x) \to \phi(x'))$. We can then use an induction axiom to deduce that $\vdash_{\mathrm{PA}} \forall x\,\phi(x)$.

By Example 3.2, $\vdash_{\mathrm{PA}} \forall x\,(\mathbf{0} + x) = x$ and, since $Q4$ is an axiom of PA, $\vdash_{\mathrm{PA}} \forall x\,(x + \mathbf{0}) = x$. Two applications of the UE Rule then enable us to deduce that $\vdash_{\mathrm{PA}} (\mathbf{0} + y) = y$ and $\vdash_{\mathrm{PA}} (y + \mathbf{0}) = y$, from which it is easy to deduce that $\vdash_{\mathrm{PA}} (\mathbf{0} + y) = (y + \mathbf{0})$ and hence, using the UI Rule, $\vdash_{\mathrm{PA}} \forall y\,(\mathbf{0} + y) = (y + \mathbf{0})$, that is $\vdash_{\mathrm{PA}} \phi(\mathbf{0})$.

Now consider the following formal proof.

1	(1)	$\forall x\,\forall y\,(x + y') = (x + y)'$	Ass
2	(2)	$\forall x\,\forall y\,(y' + x) = (y + x)'$	Ass
3	(3)	$\phi(x)$	Ass
3	(4)	$(x + y) = (y + x)$	UE, 3
1	(5)	$\forall y\,(z + y') = (z + y)'$	UE, 1
1	(6)	$(z + x') = (z + x)'$	UE, 5
1	(7)	$\forall z\,(z + x') = (z + x)'$	UI, 6
1	(8)	$(y + x') = (y + x)'$	UE, 7
2	(9)	$\forall y\,(y' + z) = (y + z)'$	UE, 2
2	(10)	$(x' + z) = (x + z)'$	UE, 9
2	(11)	$\forall z\,(x' + z) = (x + z)'$	UI, 10
2	(12)	$(x' + y) = (x + y)'$	UE, 11
2, 3	(13)	$(x' + y) = (y + x)'$	Sub, 4, 12
	(14)	$(y + x') = (y + x')$	II
1	(15)	$(y + x)' = (y + x')$	Sub, 8, 14
1, 2, 3	(16)	$(x' + y) = (y + x')$	Sub, 13, 15
1, 2, 3	(17)	$\phi(x')$	UI, 16
1, 2	(18)	$(\phi(x) \to \phi(x'))$	CP, 17
1, 2	(19)	$\forall x\,(\phi(x) \to \phi(x'))$	UI, 18

Assumption 1 is axiom $Q5$, and assumption 2 is the formula which we showed in Example 3.3 is derivable in PA. Thus we can deduce that $\vdash_{\mathrm{PA}} \forall x\,(\phi(x) \to \phi(x'))$.

Since $\vdash_{\mathrm{PA}} \phi(\mathbf{0})$ and $\vdash_{\mathrm{PA}} \forall x\,(\phi(x) \to \phi(x'))$, an application of an induction axiom shows that $\vdash_{\mathrm{PA}} \forall x\,\phi(x)$, that is $\vdash_{\mathrm{PA}} \forall x\,\forall y\,(x + y) = (y + x)$. ◆

If you have a taste for formal proofs of this kind, you may wish to attempt the following (optional) problem.

Problem 3.3

Give an outline of a formal proof to show that

$$\vdash_{\mathrm{PA}} \forall x\,\forall y\,\forall z\,((y + z) + x) = (y + (z + x))$$

3.2 Gödel's Second Incompleteness Theorem

You will remember that by Hilbert's Question we mean:

> Can the consistency of number theory be proved using only non-dubious principles of finitary reasoning?

To be able to answer this question, we need to make it precise in various ways. Firstly by *number theory* we shall mean, at least for the time being, the theory PA that we have just introduced.

In the previous subsection we gave a brief argument to justify the claim that PA is consistent. Roughly speaking, the argument for PA's consistency is as follows.

> The axioms of PA are all true in the standard interpretation $\mathscr{N}$. Since all the rules of proof are logically valid, it follows that all the theorems of PA are true in the standard interpretation. Given a sentence Φ, it cannot be that both Φ and $\neg\Phi$ are true in the standard interpretation. So Φ and $\neg\Phi$ cannot both be theorems of PA. Hence PA is consistent.

This argument does not meet Hilbert's requirements since it takes for granted the standard interpretation of number theory and the notion of 'truth' in relation to this interpretation. But the standard interpretation is an infinite mathematical object and arguments in which we assume that we have a clear notion of truth for such infinite structures go beyond 'non-dubious principles of finitary reasoning'. Indeed Gödel's First Incompleteness Theorem shows that the properties of the standard interpretation cannot be captured by any explicitly given (that is, recursive) set of axioms in our formal language. Thus our grasp of the standard interpretation is not as comprehensive as might be suggested by the consistency proof for PA given above.

We can interpret Hilbert's requirement as asking whether we can find a recursively axiomatizable theory T which is significantly weaker than PA and in which the consistency of PA can be proved. Thus we ask whether we can find a theory T such that PA is an extension of T and a sentence which expresses the consistency of PA is a theorem of T. This immediately raises the question of how we can find a sentence of the formal language which expresses the consistency of PA. The following observation is helpful.

Theorem 3.1

Let R be a theory which extends Q. Then R is consistent if and only if the sentence $\mathbf{0} = \mathbf{1}$ is not a theorem of R.

Proof

Suppose that R is a theory which extends Q. Since $\vdash_Q \neg\mathbf{0} = \mathbf{1}$ (by Theorem 2.1(b) of *Unit 7*) and R extends Q, we also have that $\vdash_R \neg\mathbf{0} = \mathbf{1}$. Thus if $\vdash_R \mathbf{0} = \mathbf{1}$, R would be inconsistent. Conversely, if R is inconsistent, then every sentence is a theorem of R (by Problem 3.2 of *Unit 6*) and hence $\vdash_R \mathbf{0} = \mathbf{1}$. ■

It follows that, to demonstrate the consistency of PA, all we need is to be able to express 'the sentence $\mathbf{0} = \mathbf{1}$ is not a theorem of PA' as a sentence of a recursively axiomizable theory T of which PA is an extension. We could do this with the sentence $\neg\theta(\ulcorner\mathbf{0} = \mathbf{1}\urcorner)$ if we had a formula θ, in which x is the only free variable, which expresses the fact that 'x is the Gödel number of a theorem of PA'.

Recall that if Φ is a sentence with Gödel number n, then $\ulcorner\Phi\urcorner$ is the term $\mathbf{n}$. Thus $\theta(\ulcorner\Phi\urcorner)$ is the sentence which results from substituting the term $\mathbf{n}$ for each free occurrence of x in θ.

The difficulty with this is that, by Theorem 1.3, provided PA is consistent, the set of Gödel numbers of the theorems of PA is not representable in PA. Thus we cannot expect to find a formula θ which represents the set of Gödel numbers of the theorems of PA. However, it is possible to construct a formula $\mathrm{Prov}(x)$, in which x is the only free variable, such that, for each sentence Φ,

$\mathrm{Prov}(\ulcorner\Phi\urcorner)$ is true in the standard interpretation if and only if $\vdash_{\mathrm{PA}} \Phi$.

The construction of the formula Prov involves a good deal of technical work, which we omit. We hope that you will take the existence of Prov on trust.

Given the formula Prov, we can restate Hilbert's Question as follows:

> Is there a recursively axiomatizable theory T such that PA is an extension of T and $\vdash_T \neg\mathrm{Prov}(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$?

We shall show that the answer to this question is 'no' by proving that, if PA is consistent, then $\neg\mathrm{Prov}(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ is not even a theorem of PA. It then immediately follows that it is not a theorem of any theory T of which PA is an extension.

Rather than prove this for the particular formula Prov, it is convenient to prove this result in a more general setting (in Theorem 3.3) which deals with any formula that might be regarded as expressing that formulas are provable in PA. We call such formulas *provability predicates.*

Definition 3.2 Provability Predicate

Let T be a theory which is an extension of Q and let θ be a formula whose only free variable is x. Then θ is called a *provability predicate* for T if the following three conditions are satisfied for all sentences Φ and Ψ.

(a) If $\vdash_T \Phi$ then $\vdash_T \theta(\ulcorner\Phi\urcorner)$.

(b) $\vdash_T (\theta(\ulcorner\Phi \to \Psi\urcorner) \to (\theta(\ulcorner\Phi\urcorner) \to \theta(\ulcorner\Psi\urcorner)))$.

(c) $\vdash_T (\theta(\ulcorner\Phi\urcorner) \to \theta(\ulcorner\theta(\ulcorner\Phi\urcorner)\urcorner))$.

If we think of $\theta(\ulcorner\Phi\urcorner)$ as expressing the fact that 'Φ is a theorem of T', we can see that the conditions in Definition 3.2 express the following statements.

(a) If Φ is a theorem of T, then we can prove in T that Φ is a theorem of T.

(b) We can prove in T that, if $(\Phi \to \Psi)$ and Φ are theorems of T, then Ψ is a theorem of T.

(c) We can prove in T that, if Φ is a theorem of T, then we can prove in T that Φ is a theorem of T.

The following theorem, interesting in its own right, which will give us our final stepping stone to answering Hilbert's Question, is proved using another very ingenious application of Gödel's Diagonal Lemma. The individual steps in the proof are not difficult to follow. They use the properties (a), (b) and (c) of a provability predicate and the Tautology Rule. The tautologies used are the following, expressed in the notation of Subsection 1.3 of *Unit 6*.

$$\text{(i)}\ \frac{\phi}{(\psi \to \phi)} \qquad \text{(ii)}\ \frac{(\phi \to \psi), \phi}{\psi} \qquad \text{(iii)}\ \frac{(\phi \to \psi), (\psi \to \chi)}{(\phi \to \chi)}$$

$$\text{(iv)}\ \frac{(\phi \to (\psi \to \chi)), (\phi \to \psi)}{(\phi \to \chi)} \qquad \text{(v)}\ \frac{(\phi \leftrightarrow \psi), \psi}{\phi}$$

Tautologies (ii) and (iii) are the standard tautological consequences 8 and 10 given in Subsection 1.3 of *Unit 6*.

We realize that the proof as a whole is rather difficult to grasp, so you should not worry if you find it hard to see what is really going on. We shall not expect you to remember either the theorem or its proof, but we have included it so that you can see what is involved in answering Hilbert's Question.

Theorem 3.2 Löb's Theorem

Let T be a theory which extends Q and let θ be a provability predicate for T. Then, for each sentence Φ, $\vdash_T \Phi$ if and only if $\vdash_T (\theta(\ulcorner\Phi\urcorner) \to \Phi)$.

This theorem was proved by M.H. Löb in 1955.

Proof

Suppose that T is a theory which extends Q and that θ is a provability predicate for T. Let Φ be a sentence.

If $\vdash_T \Phi$ then by the Tautology Rule (using tautology (i)) $\vdash_T (\theta(\ulcorner\Phi\urcorner) \to \Phi)$.

Conversely, suppose that

$$\vdash_T (\theta(\ulcorner\Phi\urcorner) \to \Phi) \tag{3.5}$$

Let $\delta(x)$ be the formula $(\theta(x) \to \Phi)$ in which x is the only variable which may occur freely. Since T is an extension of Q, the function diag is representable in T, and so we can apply Gödel's Diagonal Lemma (Theorem 3.5 of *Unit 7*) to deduce that there is a sentence G_δ such that $\vdash_T (G_\delta \leftrightarrow \delta(\ulcorner G_\delta\urcorner))$, that is

We met the function diag and saw that it is representable in any theory that extends Q in Subsection 3.2 of *Unit 7*.

$$\vdash_T (G_\delta \leftrightarrow (\theta(\ulcorner G_\delta\urcorner) \to \Phi)) \tag{3.6}$$

and hence

$$\vdash_T (G_\delta \to (\theta(\ulcorner G_\delta\urcorner) \to \Phi)) \tag{3.7}$$

Using property (a) of a provability predicate, (3.7) gives

$$\vdash_T \theta(\ulcorner(G_\delta \to (\theta(\ulcorner G_\delta\urcorner) \to \Phi))\urcorner) \tag{3.8}$$

Now, by property (b) of a provability predicate, we have

$$\vdash_T (\theta(\ulcorner(G_\delta \to (\theta(\ulcorner G_\delta\urcorner) \to \Phi))\urcorner) \to (\theta(\ulcorner G_\delta\urcorner) \to \theta(\ulcorner(\theta(\ulcorner G_\delta\urcorner) \to \Phi)\urcorner))) \tag{3.9}$$

The Tautology Rule applied to (3.8) and (3.9) (tautology (ii)) gives

$$\vdash_T (\theta(\ulcorner G_\delta\urcorner) \to \theta(\ulcorner(\theta(\ulcorner G_\delta\urcorner) \to \Phi)\urcorner)) \tag{3.10}$$

Using property (b) again, we have

$$\vdash_T (\theta(\ulcorner(\theta(\ulcorner G_\delta\urcorner) \to \Phi)\urcorner) \to (\theta(\ulcorner\theta(\ulcorner G_\delta\urcorner)\urcorner) \to \theta(\ulcorner\Phi\urcorner))) \tag{3.11}$$

The Tautology Rule applied to (3.10) and (3.11) (tautology (iii)) gives

$$\vdash_T (\theta(\ulcorner G_\delta\urcorner) \to (\theta(\ulcorner\theta(\ulcorner G_\delta\urcorner)\urcorner) \to \theta(\ulcorner\Phi\urcorner))) \tag{3.12}$$

By property (c) of a provability predicate, we have

$$\vdash_T (\theta(\ulcorner G_\delta\urcorner) \to \theta(\ulcorner\theta(\ulcorner G_\delta\urcorner)\urcorner)) \tag{3.13}$$

The Tautology Rule applied to (3.12) and (3.13) (tautology (iv)) gives

$$\vdash_T (\theta(\ulcorner G_\delta\urcorner) \to \theta(\ulcorner\Phi\urcorner)) \tag{3.14}$$

Now the Tautology Rule applied to (3.5) and (3.14) (tautology (iii)) gives

$$\vdash_T (\theta(\ulcorner G_\delta\urcorner) \to \Phi) \tag{3.15}$$

We can now apply the Tautology Rule to (3.6) and (3.15) (tautology (v)) to deduce that

$$\vdash_T G_\delta \tag{3.16}$$

Hence, by property (a) of a provability predicate, (3.16) gives

$$\vdash_T \theta(\ulcorner G_\delta\urcorner) \tag{3.17}$$

Finally from (3.15) and (3.17) and another application of the Tautology Rule (tautology (ii)), we can deduce that

$$\vdash_T \Phi \tag{3.18}$$

We have thus shown that (3.5) implies (3.18), completing the proof. ■

This theorem leads immediately to the result we need.

Theorem 3.3

If T is a consistent extension of Q and θ is a provability predicate for T then $\neg\theta(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ is not a theorem of T.

Proof

Suppose that T is a consistent extension of Q and that θ is a provability predicate for T.

Now assume that

$$\vdash_T \neg\theta(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$$

By an application of the Tautology Rule, using the tautology $(\neg\phi \rightarrow (\phi \rightarrow \psi))$, it follows that

$$\vdash_T (\theta(\ulcorner \mathbf{0} = \mathbf{1} \urcorner) \rightarrow \mathbf{0} = \mathbf{1})$$

Hence, by Theorem 3.2,

$$\vdash_T \mathbf{0} = \mathbf{1}$$

Now, as T is an extension of Q, it follows, by Theorem 3.1, that T is not consistent. From this contradiction we can deduce that $\neg\theta(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ cannot be a theorem of T. ■

We wish to use Theorem 3.3 to show that, if PA is consistent, then $\neg\mathrm{Prov}(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ is not a theorem of PA. To be able to draw this conclusion, we need to know that Prov is a provability predicate for PA. The detailed verification of this is complicated, so we hope you will take it on trust that

Prov is a provability predicate for PA.

It is worth remarking that here we really do need a powerful theory with lots of axioms such as PA. For Prov to be a provability predicate, we need to know that conditions (a), (b) and (c) of Definition 3.2 hold, and this requires that the sentences given in these conditions are theorems of our theory. For this to be true, a powerful theory is needed. The analogous result for a weak theory such as Q would not hold.

Theorem 3.4 Gödel's Second Incompleteness Theorem

If Peano Arithmetic, PA, is consistent, then $\neg\mathrm{Prov}(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ is not a theorem of PA.

Proof

Since PA is an extension of Q, and Prov is a provability predicate for PA, this is an immediate consequence of Theorem 3.3. ■

We have included the hypothesis that PA is consistent in our statement of Theorem 3.4 since its main interest stems from Hilbert's Question, and this question has little significance if the consistency of PA is taken for granted. However, if we do accept the existence of the standard interpretation $\mathscr{N}$ and hence the consistency of PA, then $\neg\mathrm{Prov}(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ is a true sentence (in the standard interpretation). Thus $\neg\mathrm{Prov}(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ is an example of a true sentence that is not a theorem of PA. Since the sentence $\mathrm{Prov}(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ is false, then it is also not a theorem of PA. So we obtain an example of a sentence Φ such that neither $\vdash_{\mathrm{PA}} \Phi$ nor $\vdash_{\mathrm{PA}} \neg\Phi$ and thus a direct example to show that the theory PA is not complete. This is essentially the proof that Gödel gave of his First Incompleteness Theorem.

Now we are in a position to answer Hilbert's Question, at least in the way we have reformulated it. Taking together Theorems 3.1 and 3.4 we can conclude that

if PA is consistent, then we cannot prove in PA that it is consistent.

So our answer to Hilbert's Question is 'no'.

Despite this answer, since almost all mathematicians believe that they have a clear and coherent concept of the natural numbers and hence of what we have called the standard interpretation, the consistency of the theory PA is not seriously in doubt. However, note that Theorem 3.3 applies to all theories which extend PA, and this includes *theories of infinite sets* which are very much more powerful than PA. For these powerful set theories there is no standard interpretation, or indeed any other interpretation, of which it is plausible to claim that we have a very clear conception. Thus the possibility that such theories are inconsistent needs to be taken seriously. The absence of finitary consistency proofs for such theories therefore has great philosophical significance. It shows that Hilbert's idea for securing the consistency of the mathematics of the infinite cannot be accomplished.

BIOGRAPHICAL SKETCHES

In this section we give some brief biographical sketches of some of the mathematicians and logicians we have mentioned earlier in the course.

Cantor

Georg Cantor (1845–1918) was born to German parents in St Petersburg, Russia. His father was a successful Protestant merchant, his mother a Catholic; religion was to play an increasing role in Cantor's life as he grew older. He studied mathematics at Berlin University, where he was attracted to the rigorous approach to analysis advocated by Karl Weierstrass.

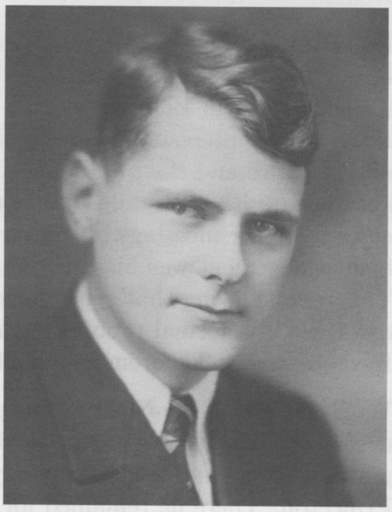
His first significant research was on the convergence of trigonometric series, where he was led to the delicate study of point sets on the real line, which later influenced his ideas about ordinal numbers. In 1871 he began a long correspondence with Richard Dedekind, in which he showed that the rational numbers formed a countable set but the real numbers formed a strictly larger, uncountable set. Since Cantor had also shown that the set of algebraic numbers is countable, this immediately implied the existence of uncountably many transcendental numbers.

Cantor went on to explore the new world of uncountable sets. He showed, for example, that there was a one-to-one correspondence between the points of an interval and a square, which seemed to imperil the concept of dimension, and was led to conjecture that any infinite subset of the real numbers can be put in a one-to-one correspondence with either the set of natural numbers or the set of real numbers. This is the famous continuum hypothesis, unproved to this day, despite modern set theory being considerably more precise than it was in Cantor's time.

Cantor may also have been the first to discover the paradoxes of the largest cardinal and the largest ordinal. The first follows from the facts that every set has a cardinality, and the 'set' of all cardinals has a cardinality larger than any cardinal. The paradox of the 'set' of all ordinals is similar. The resolution of the paradoxes, when they began to cause concern in the 1900s, has generally been taken to lie in realizing that not all collections can form sets; but Cantor seems to have regarded them with equanimity because they appealed to his ideas about the truly infinite and the nature of God.

Cantor spent all his working life as a professor at the small University of Halle, hoping for a call that never came from the University of Berlin. He seems to have been devoted to his family, but suffered a number of periods of acute mental illness. Cantor's work did not get the recognition it deserved from some of his contemporaries, who did not accept the validity of his theory of infinite sets. However, the younger generation of mathematicians, led by David Hilbert, regarded set theory as a mathematical paradise and the proper place for the foundation of all mathematics.

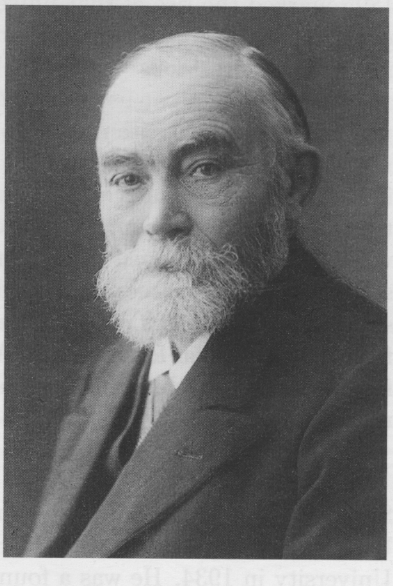
Church



Alonzo Church (Photo © the estate of Alonzo Church)

Alonzo Church (1903–1995) was born in Washington DC in the USA and spent much of his professional life at Princeton University, where he obtained both his bachelor and PhD degrees and then served as a professor from 1929 to 1967. He produced work of major importance in logic, recursion theory and computer science, publishing his first paper in 1924 and his last in 1995, the year he died. His achievements include his work on recursive functions leading to his proposal of what became known as Church's Thesis, his proof that there is no algorithm for deciding which sentences of quantifier logic are logically valid, and his creation of the lambda calculus. He was the doctoral supervisor of many of the most distinguished logicians of the twentieth century, including Stephen Kleene and Alan Turing. He was known for his extreme precision when lecturing. His *Introduction to Mathematical Logic*, published in 1956, which also shows great care with the details, has proved to be a very influential textbook. He further fostered the study of logic as co-founder of the Association of Symbolic Logic in 1936 and by playing a leading role in running for many years the *Journal of Symbolic Logic*, the premier learned journal devoted to mathematical logic.

Frege



Gottlob Frege (Photo courtesy of the Friedrich-Schiller-University, Jena)

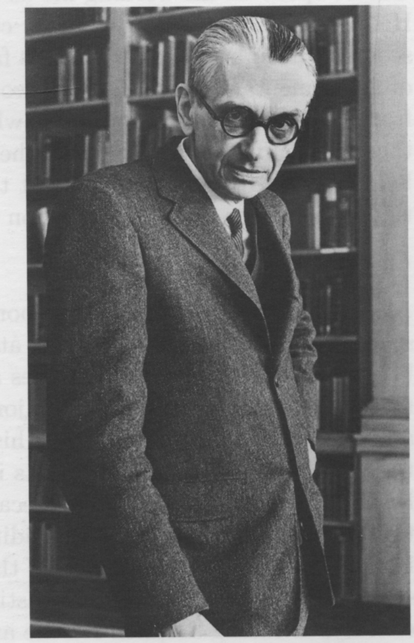
Gottlob Frege (1848–1925) became a student at Jena University in 1869. He moved to Gottingen University in 1871 and was awarded a PhD in 1873. He then returned to Jena University where he taught mathematics for forty-four years and was known as clear, conscientious and demanding teacher. His research concentrated more and more on the foundations of mathematics. Frege came to believe that the basic concepts of mathematics, with the possible exception of geometry, could be defined in purely logical terms, and theorems could then be derived using just logical reasoning. To justify this claim, in his *Begriffsschrift* (Conceptual Notation) of 1879 he described a formal system in which deductions were carried out. This was the first published system of quantifier logic and Frege merits great credit for his invention. Unfortunately he chose an awkward notation and this restricted the influence of his book.

After describing his philosophical ideas informally in *Die Grundlagen der Arithmetik* (The Foundations of Mathematics) in 1884, he began work on *Die Grundgesetze der Arithmetik* (The Basic Laws of Arithmetic), which was intended to be his definitive account of how theorems of number theory and mathematical analysis may be derived within his formal system. The first volume was published in 1893. However, in June 1902, just as the second volume was nearing completion, he received a letter from Bertrand Russell drawing his attention to a contradiction, now called Russell's Paradox, which Russell had derived within Frege's system. To his great credit, Frege, who had indulged in polemics much of his working life, gracefully acknowledged the force of Russell's criticism. He was never able to repair the damage and towards the end of his life he seems to have abandoned his belief that number could be derived purely from logic.

Frege's work won little attention in his lifetime, but he is now regarded as a founder of mathematical logic and as a great philosopher of mathematics and logic.

Gödel

Kurt Gödel (1906–1978), who was a native of Brno (in modern-day Czech Republic), who studied mathematics at the University of Vienna and took his PhD there in 1930. One of his main teachers of mathematics was Hans Hahn whose interests included point-set topology, the foundations of mathematics and the philosophy of science. Hahn introduced Gödel to a group of positivistic philosophers now known as the Vienna Circle. Gödel attended their meetings but never accepted their philosophical ideas. His first achievement was his theorem, which we have called the Adequacy Theorem, showing that every logically valid formula in first-order logic is derivable in a formal proof system. He first presented his First Incompleteness Theorem at a conference in Königsberg when he was 24.



Kurt Gödel (Photo courtesy of the Archives of the Institute for Advanced Study)

With the rise of the Nazis it was prudent for him to emigrate, and he eventually reached America, via Russia, in 1940, when he took up a permanent position at the recently founded Institute for Advanced Study in Princeton. There he remained for the rest of his life. He worked at first on set theory and in 1938 published a proof that if the standard axiom system for set theory is consistent then Cantor's continuum hypothesis cannot be disproved in the system. He became a good friend of Albert Einstein, who was also a professor at the Institute, and even discovered a novel space-time that seems to allow the possibility of time travel. In his final years he became a complete recluse, and starved to death in 1978 because of his fear of consuming harmful germs.

Hilbert

Königsberg is today called Kaliningrad and is in Russia.

David Hilbert (1862–1943) was born and studied in Königsberg in East Prussia and became a professor there in 1892. His transfer to Göttingen in 1895 marked the rise of that university to become the leading centre for mathematics in the world. Hilbert's remarkable mathematical ability showed itself in the late 1880s when he solved a famously difficult problem in algebra, making great use of a non-constructive existence argument (which proved to be a favourite method of his). He worked on numerous branches of mathematics: number theory, functional analysis, and mathematical physics including general relativity. He was a passionate advocate of Cantorian set theory, and of the axiomatic approach to pure, and applied, mathematics, which he first developed in the context of elementary geometry. In the second half of his career, he hoped to create a combined version of logic and set theory from which could be derived all of mathematics in a rigorous way from simple logical foundations. Although he failed in this, many of the fragments of his achievement remained for later mathematical logicians to refine.

Kleene

Stephen Kleene (1909–1994) — the name is pronounced clay-nee — was born in Hartford, Connecticut, USA, and took his PhD at Princeton University in 1934. He was a founder of modern recursion theory, and in 1983 he was awarded the American Mathematical Society's Steele Prize for his seminal papers of 1955 on recursion theory and descriptive set theory. He taught for most of his life at the University of Wisconsin–Madison, where he built up a large school of logicians in the Mathematics Department. Among his influential papers and books are his *Introduction to Metamathematics* (1952) and *Mathematical Logic* (1962). In 1990 Kleene was awarded the President's National Medal of Science, America's highest scientific honour, for his leadership in the theory of recursion and effective computability and for developing it into a deep and broad field of mathematical research. He was also a keen mountaineer and an energetic conservationist.

Leibniz

Gottfried Wilhelm Leibniz (1646–1716) was, with Isaac Newton, the commanding mathematician of his time, though most of his working life was spent working for the Duke of Brunswick on a genealogy project that prevented his remarkable talents from exerting their full influence. His own discovery of the fundamental ideas of the calculus came in the late 1670s, some years after Newton's discovery, which was at that time unpublished. Leibniz's interests in philosophy were profound, and he also held out hopes for a universal language and for a language in which all ideas could be expressed and all disputes resolved by calculation. He could not match Newton when it came to applying mathematics to the study of nature, but he surpassed him in extending the techniques of the calculus and in passing it to the next generation through his correspondence with the Bernoulli brothers Johann and Jakob. In the late nineteenth century many of his hitherto unpublished ideas on logic and metaphysics were made available for the first time in scholarly editions, and became a rallying point for Frege, Russell and others.

Peano

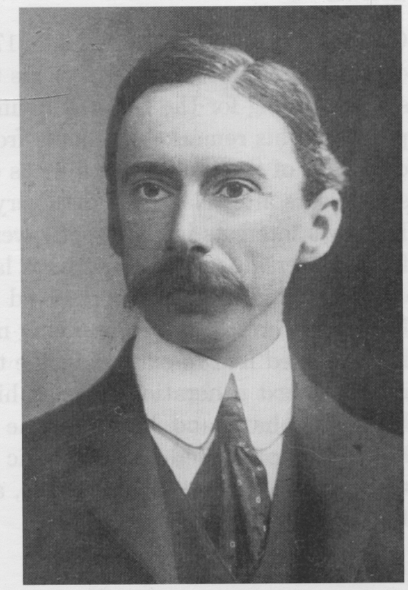
Giuseppe Peano (1858–1932) was an Italian mathematician who taught almost all his life at the University of Turin. He opposed the sweeping use of geometrical arguments and instead preferred careful analytic arguments often tending to seemingly paradoxical conclusions, such as his discovery of a continuous map of the unit interval onto the unit square, the first example of a space-filling curve. He proceeded to introduce much of the now-standard notation in logic and set theory, which is what commended him to Bertrand Russell, and to advocate a form of simplified Latin for use in all scientific work (and indeed, more generally, as an alternative to Esperanto). For a time he inspired a group of Italian mathematicians and logicians, but after the First World War he was an increasingly isolated figure.

Apart from his other contributions to mathematics, Peano is renowned for his skill in devising good notation. It is Peano to whom we are indebted for, for instance, the symbol $\in$ for set membership. In his autobiography, Bertrand Russell wrote that the International Congress of Philosophy in Paris in 1900 'was a turning point in my intellectual life, because I there met Peano .... It became clear to me that his notation afforded an instrument of logical analysis such as I had been seeking for years, and that by studying him I was acquiring a new and powerful technique for the work I had long wanted to do.'

Post

Emil Post (1897–1954) was born into a Jewish family in Poland in 1897 and emigrated with his parents to New York in 1904. He studied mathematics at City College and took his PhD from Columbia University, New York, in 1920. He lost an arm in an accident as a child, and suffered all his adult life from crippling manic depression, which prevented him from obtaining a permanent position until 1935 when he became a professor at City College, where he remained until he died in 1954. Post first studied logic at a seminar at Columbia University as a graduate student. In his thesis he isolated the propositional logic part of Russell and Whitehead's *Principia Mathematica* and used the method of truth tables to show it was consistent and complete. He regarded systems of logic as systems of finitary symbol manipulation, and in later work came close to Gödel's Incompleteness Theorems. In 1943 he lectured to the American Mathematical Society on the field of recursive unsolvability — probably his most influential achievement — and his theorems in this area have inspired other proofs of unsolvability in the theory of formal languages.

Russell



Bertrand Russell (Photo © Mary Evans Picture Library)

Bertrand Russell (1872–1970) was born into an aristocratic family. He studied mathematics and philosophy as a student at Trinity College, Cambridge. He won a fellowship in 1895 for an essay subsequently published as *An Essay on the Foundations of Geometry.* His interest in the philosophy of mathematics was enhanced by a meeting with Giuseppe Peano in 1900. Independently of Gottlob Frege, Russell came to the view that mathematics could be reduced to logic. This thesis is put forward in his *Principles of Mathematics* which he began writing in 1900 but which was not published until 1903. During this period he got to know of Frege's work, and he also discovered the paradox now known as Russell's Paradox.

Russell planned to follow *Principles of Mathematics* with a second volume in which his claim that all the theorems of pure mathematics are deducible using 'a small number of fundamental logic principles' would be established 'by strict symbolic reasoning'. To achieve this aim Russell collaborated with the Cambridge mathematician Alfred North Whitehead, and their *Principia Mathematica* was published in three volumes between 1910 and 1913. In this work Russell's Paradox was avoided by using Russell's Theory of Types. This makes the logical system complicated and undermines the claim that mathematics has been deduced from 'small number of fundamental logical principles'.

Russell courageously opposed the First World War. His political activities led to the loss in 1916 of his lectureship at Trinity College, and to his being jailed in 1918 for publishing a seditious pamphlet. After publishing *Principia Mathematica* he only rarely returned to serious work in mathematical logic. Towards the end of his life he became active in the campaign against nuclear weapons and in 1961 he was imprisoned again for short period.

Turing

Alan Mathison Turing (1912–1954) studied mathematics at King's College, Cambridge, where he developed an interest in logic. In 1936 he gave the first proof of an algorithmically unsolvable problem when he showed that the Halting Problem is algorithmically undecidable (Theorem 3.1 of *Unit 3*). In the course of this work he devised the notion of a Turing machine, a particularly clear way of describing an automated reasoning process. During the Second World War he was very influential in the code-breaking efforts centred at Bletchley Park, and this led to work on electronic computers that he later continued at the University of Manchester. In March 1952 he was charged with committing homosexual acts which were then illegal. He pleaded guilty and was put on probation subject to the condition that he undertook a course of hormone injections that were supposed to reduce his homosexual urges. He committed suicide on 7 June 1954 by eating an apple laced with cyanide.

SUGGESTIONS FOR FURTHER READING

Because of the great significance of Gödel's Incompleteness Theorems, the literature on the subject is vast. We give only a selection of books. They are a mixture of works of historical or biographical interest and some textbooks which present the proofs of Gödel's theorems and related results.

With the exception of Gödel's original paper, we restrict ourselves to works in English. There are lots of different, but equivalent, ways of presenting systems of formal logic. So if you look at any of the books listed here, you must be prepared for differences in notation and presentation.

The details of the books mentioned are in the bibliography given at the end. We give references to this bibliography in the form [n], where n is the number of the book in the bibliography.

Most of these books should be available in a good academic library. Public libraries should be able to obtain them through the inter-library loan system.

Recursive functions, Turing machines and URMs

Alan Turing's original paper is [29]. This is reprinted in [7] and [13]. The original paper in which URMs were described is [25]. Our treatment of URMs follows very closely that of Nigel Cutland [4]. Note, however, that we have used $C(m, n)$ for Copy instructions whereas Cutland uses $T(m, n)$. Also we have used a different system for assigning code numbers to URM programs and URM computations so as to bring it into line with our method of assigning Gödel numbers to formulas. For a detailed treatment of computable functions in terms of Turing machines see [6]. Recursive functions are also covered in [10], [16], [18] and [19].

Formal systems of logic

Church's book [3] is a classic text which covers propositional and quantifier logic in great detail, but which covers neither recursive functions nor Gödel's theorems (a promised second volume covering them never appeared). Kleene's book [18] is another classic text which does include recursive functions and Gödel's theorems.

Both these influential textbooks are hard going for beginners. There is now available a large number of more accessible introductions to mathematical logic. We have chosen to recommend [10], [16] and [19]. Each of these books has stood the test of time. They all give a more detailed introduction to propositional and quantifier logic than we have had space for. In particular they all give proofs of the Correctness Theorem and the Adequacy Theorem for quantifier logic, which we omitted. They also cover recursive functions and Gödel's Incompleteness Theorems, and give proofs of the representability of total recursive functions in sufficiently powerful systems of formal arithmetic, which we did not give in full.

The Correctness Theorem is called the Soundness Theorem in [10] and [16] and is unnamed in [19]. The Adequacy Theorem is called the Completeness Theorem in [10] and [19].

Gödel's Incompleteness Theorems

Gödel's original paper is [14]. English translations are given in [15] (which also includes the original German text), [7], [24] and [30]. Each of these volumes is also of separate interest.

The first volume of Gödel's *Collected Works* [15] includes a biographical sketch of Gödel by John Dawson and a useful introductory note about Gödel's paper by Kleene. [7] is a collection of reprints of some important papers which also includes Turing's paper [29] and the paper in which Church first put forward what we have called Church's Thesis. The volume [24] edited by S.G. Shanker includes a selection of philosophical and historical papers commenting on the reception of Gödel's theorems and their philosophical significance. The volume [30] edited by Jean van Heijenoort is a very scholarly volume consisting of key papers in mathematical logic with useful editorial introductions.

An advanced, but none the less very readable, book illustrating further some of the strong connections between the number theory and mathematical logic encountered in this course is [26]. Another advanced but still very readable book on computability and logic, giving further interesting historical background, is [11].

Two amusing and challenging books of logic puzzles by the logician (and magician) Raymond Smullyan, which lead to discussions of Gödel's theorems and what we have called Leibniz's Question, are [27] and [28].

Biographies

Martin Davis's book [8] is an entertaining short history describing some of the pathway connecting the ideas of Leibniz with the work of Gödel and Turing. The book by E.J. Aiton [2] is an accessible biography of Leibniz. Probably the most accessible source of biographical information about Cantor is [1]. J.W. Dauben's book [5] is a more scholarly account of Cantor's work with some biographical information. Many of Frege's papers were destroyed during the Second World War and as a consequence many details of his life are not known. Our biographical comments are based on Terrell Ward Bynum's biography in [12]. This volume also includes a translation of Frege's *Begriffsschrift*, as also does [30]. Constance Reid's book [22] is a very readable account of the life and work of Hilbert. The lives of Gödel and Turing are covered in [9] and [17]. Russell wrote an interesting but not always reliable or balanced autobiography [23]. He has attracted the interest of several biographers: the two-volume biography by Ray Monk [20], [21] is perhaps the best, and not always favourable to Russell.

Bibliography

The dates given are normally those of the first edition of each book, many of which have been subsequently reprinted.

1. Amir D. Aczel, *The Mystery of the Aleph*, Washington Square Press, 2000.
2. E.J. Aiton, *Leibniz: a Biography*, Adam Hilger, 1985.
3. Alonzo Church, *Introduction to Mathematical Logic, volume 1*, Princeton University Press, 1956.
4. Nigel Cutland, *Computability*, Cambridge University Press, 1980.
5. J.W. Dauben, *Georg Cantor*, Princeton University Press, 1990.
6. Martin Davis, *Computability and Unsolvability*, McGraw-Hill, 1958.
7. Martin Davis (editor), *The Undecidable*, Raven Press, 1965.
8. Martin Davis, *The Universal Computer: the Road from Leibniz to Turing*, W.W. Norton, 2000.
9. John Dawson, *Logical Dilemmas: the Life and Work of Kurt Gödel*, A.K. Peters, 1997.
10. Herbert B. Enderton, *A Mathematical Introduction to Logic*, second edition, Academic Press, 2001.
11. R.L. Epstein and W.A. Carnielli, *Computability: Computable Functions, Logic and the Foundations of Mathematics*, Wadsworth, 1989.
12. Gottlob Frege, *Conceptual Notation and Related Articles*, translated and edited with a Biography and Introduction by Terrell Ward Bynum, Clarendon Press, 1972.
13. R.O. Gandy and C.E.M. Yates (editors), *Collected Works of A.M. Turing: Mathematical Logic*, Elsevier, 2001.
14. Kurt Gödel, 'Über formal unentscheidbare Sätze per Principia Mathematica und verwandter Systeme I', *Monatshefte für Mathematik und Physik*, volume 38, 1931, pages 173–198.
15. Kurt Gödel, *Collected Works, volume 1*, edited by Solomon Feferman *et al*, Oxford University Press, 1986.
16. A.G. Hamilton, *Logic for Mathematicians*, Cambridge University Press, 1978.
17. Andrew Hodges, *Alan Turing: the Enigma*, Burnett Books, 1983.
18. Stephen Cole Kleene, *Introduction to Metamathematics*, North-Holland, 1952
19. Elliott Mendelson, *Introduction to Mathematical Logic*, Van Nostrand, 1964.

20. Ray Monk, *Bertrand Russell: The Spirit of Solitude*, Jonathan Cape, 1996.
21. Ray Monk, *Bertrand Russell: The Ghost of Madness*, Jonathan Cape, 2000.
22. Constance Reid, *Hilbert*, George Allen & Unwin/Springer Verlag, 1970.
23. Bertrand Russell, *The Autobiography of Bertrand Russell*, three volumes, George Allen & Unwin, 1967, 1968 and 1969.
24. S.G. Shanker (editor), *Gödel's Theorem in Focus*, Croom Helm, 1988.
25. J.C. Shepherdson and H.E. Sturgis, 'Computability of recursive functions', *Journal of the Association of Computing Machinery*, volume 10, 1963, pages 217–255.
26. Craig Smoryński, *Logical Number Theory, volume 1*, Springer Verlag, 1991.
27. Raymond Smullyan, *What is the Name of this Book?*, Pelican, 1981.
28. Raymond Smullyan, *The Lady or the Tiger*, Pelican, 1983.
29. A.M. Turing, 'On computable numbers, with an application to the Entscheidungsproblem', *Proceedings of the London Mathematical Society*, series 2, volume 42, 1936–37, pages 230–265.
30. Jean van Heijenoort (editor), *From Frege to Gödel: a Source Book in Mathematical Logic*, Harvard University Press, 1967.

SUMMARY

In this unit we obtained answers to the questions which we posed at the beginning of *Unit 1*, Leibniz's Question and Hilbert's Question.

First we exploited Gödel's Diagonal Lemma to prove that, for any consistent theory T which extends Q, the set $GN(T)$ of Gödel numbers of theorems of T is not representable in T. We then exploited this result to show that the set of Gödel numbers of the sentences true in the standard interpretation $\mathscr{N}$ is not recursive. Given the evidence for Church's Thesis, which identifies the notions of algorithmically computable function and recursive function, this means that there is no algorithm for deciding which statements of number theory are true, thus providing a negative answer to Leibniz's Question.

We then asked whether there is a set of axioms for the theory Complete Arithmetic (CA) for which there is an algorithm to decide whether any given formula is one of the axioms. The existence of such a set of axioms would have led to a way of deciding whether a given sequence of formulas was a correct formal proof within the theory CA. This led to a discussion of the ideas of a *recursively axiomatizable* theory and a *recursively enumerable* set of natural numbers. Using these ideas we proved Gödel's First Incompleteness Theorem which states that there is no complete and consistent recursively axiomatizable extension of Q. Thus, in particular, CA is not recursively axiomatizable.

Finally we introduced the theory *Peano Arithmetic* (PA) which is recursively axiomatizable and from which a significant portion of number theory can be derived. We discussed the idea of a *provability predicate* of a theory. Using, in particular, the provability predicate Prov for PA we proved Gödel's Second Incompleteness Theorem which shows that the sentence $\neg\mathrm{Prov}(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ is not a theorem of PA. In the standard interpretation this sentence essentially asserts that the theory PA is consistent. The impossibility of deriving this sentence in the theory PA gives a negative answer to Hilbert's Question.

OBJECTIVES

We list topics on which we may set examination questions to test your understanding of this unit.

After working through the unit you should be able to explain the meaning of each of the following results (and thus of the technical terms used in stating them) and how they relate to Leibniz's and Hilbert's Questions.

(a) *Theorem 1.3*
Let T be a consistent theory which extends Q. Then the set $GN(T)$ of Gödel numbers of the theorems of T is not representable in T.

(b) *Theorem 1.4 Negative Answer to Leibniz's Question*
The set of Gödel numbers of the sentences which are true in the standard interpretation $\mathscr{N}$ is not recursive, or equivalently there is no algorithm for deciding which statements of number theory are true.

(c) *Theorem 1.5*
Let T be a consistent theory which extends Q. Then the set of the Gödel numbers of the sentences which are theorems of T is not recursive.

(d) *Theorem 1.6*
There is no algorithm for deciding which sentences are theorems of Q.

(e) *Theorem 1.9 Church's Theorem*
There is no algorithm for deciding which sentences of quantifier logic are logically valid.

(f) *Theorem 2.1*
The set $GN(T)$ of Gödel numbers of the theorems of a recursively axiomatizable theory T form a recursively enumerable set.

(g) *Theorem 2.2*
A complete recursively axiomatizable theory has a recursive set of theorems.

(h) *Theorem 2.3 Gödel's First Incompleteness Theorem*
There is no complete and consistent recursively axiomatizable extension of Q.

(i) *Theorem 2.4*
Complete Arithmetic is not recursively axiomatizable.

(j) *Theorem 3.4 Gödel's Second Incompleteness Theorem*
If Peano Arithmetic, PA, is consistent, then $\neg\mathrm{Prov}(\ulcorner \mathbf{0} = \mathbf{1} \urcorner)$ is not a theorem of PA, thus providing a negative answer to Hilbert's Question.

We shall not test your understanding of the *proofs* of these theorems.

SOLUTIONS TO THE PROBLEMS

Solution 1.1

Suppose that δ_A is a formula with x as its only free variable, such that (a) if $n \in A$ then $\vdash_T \delta_A(\mathbf{n})$ and (b) if $n \notin A$ then $\vdash_T \neg\delta_A(\mathbf{n})$.

Let ϕ_A be the formula

$$((\delta_A(x) \mathbin{\&} y = \mathbf{1}) \vee (\neg\delta_A(x) \mathbin{\&} y = \mathbf{0}))$$

We show that ϕ_A represents the characteristic function χ_A of A in the theory T.

Take $n, k \in \mathbb{N}$ and suppose that $\chi_A(n) = k$.

We consider first the case where $n \in A$, in which case $k = 1$.

Since $n \in A$, $\vdash_T \delta_A(\mathbf{n})$. By the II Rule $\vdash_T \mathbf{1} = \mathbf{1}$. Hence, using the Tautology Rule, it follows that

$$\vdash_T ((\delta_A(\mathbf{n}) \mathbin{\&} \mathbf{1} = \mathbf{1}) \vee (\neg\delta_A(\mathbf{n}) \mathbin{\&} \mathbf{1} = \mathbf{0}))$$

that is $\vdash_T \phi_A(\mathbf{n}, \mathbf{1})$. Hence, as $k = 1$, we have

$$\vdash_T \phi_A(\mathbf{n}, \mathbf{k})$$

and so the first condition for representability is satisfied by ϕ_A when $n \in A$.

Since $\vdash_T \delta_A(\mathbf{n})$, using the Tautology Rule we have that

$$\vdash_T (((\delta_A(\mathbf{n}) \mathbin{\&} y = \mathbf{1}) \vee (\neg\delta_A(\mathbf{n}) \mathbin{\&} y = \mathbf{0})) \rightarrow y = \mathbf{1})$$

Here we use the fact that the formula $(\gamma \rightarrow (((\gamma \mathbin{\&} \psi) \vee (\neg\gamma \mathbin{\&} \chi)) \rightarrow \psi))$ is a tautology.

Thus we have

$$\vdash_T (\phi_A(\mathbf{n}, y) \rightarrow y = \mathbf{1})$$

Hence, using the UI Rule,

$$\vdash_T \forall y\, (\phi_A(\mathbf{n}, y) \rightarrow y = \mathbf{1})$$

that is, since $k = 1$,

$$\vdash_T \forall y\, (\phi_A(\mathbf{n}, y) \rightarrow y = \mathbf{k})$$

and so the second condition for representability is satisfied by ϕ_A when $n \in A$.

The case where $n \notin A$ and $k = 0$ is similar.

So both conditions for representability are satisfied by ϕ_A in both cases. Hence ϕ_A represents χ_A in T.

Solution 1.2

In using the Tautology Rule to deduce (1.8) from (1.5) and (1.7), we used the fact that $\neg\phi$ is a tautological consequence of $(\phi \leftrightarrow \neg\psi)$ and ψ, where ϕ is the formula G and ψ is $\theta_T(\ulcorner G \urcorner)$. For this to be a correct use of the Tautology Rule we need to check that

$$(((\phi \leftrightarrow \neg\psi) \mathbin{\&} \psi) \rightarrow \neg\phi)$$

is a tautology, which is easily seen from its truth table.

$(((\phi$	$\leftrightarrow$	$\neg$	$\psi)$	$\&$	$\psi)$	$\rightarrow$	$\neg$	$\phi)$
1	0	0	1	0	1	1	0	1
1	1	1	0	0	0	1	0	1
0	1	0	1	1	1	1	1	0
0	0	1	0	0	0	1	1	0

In using the Tautology Rule to deduce (1.11) from (1.5) and (1.10), we used the fact that ϕ is a tautological consequence of $(\phi \leftrightarrow \neg\psi)$ and $\neg\psi$. To check that this is a correct use of the Tautology Rule we need to check that

$$(((\phi \leftrightarrow \neg\psi)\ \&\ \neg\psi) \rightarrow \phi)$$

is a tautology, which is easily seen from its truth table.

$(((\phi$	$\leftrightarrow$	$\neg$	$\psi)$	$\&$	$\neg$	$\psi)$	$\rightarrow$	$\phi)$
1	0	0	1	0	0	1	1	1
1	1	1	0	1	1	0	1	1
0	1	0	1	0	0	1	1	0
0	0	1	0	0	1	0	1	0

Solution 2.1

One suitable recursive function f for enumerating the set is given by

$$f(n) = \begin{cases} 2, & \text{if } n = 2, \\ 3, & \text{if } n = 3, \\ 8, & \text{otherwise.} \end{cases}$$

This f gives the values

$$\{f(0), f(1), f(2), f(3), f(4), f(5), \ldots\} = \{8, 8, 2, 3, 8, 8, \ldots\} = \{2, 3, 8\}.$$

The function f is of the form

$$f(n) = \begin{cases} g_1(n), & \text{if } R_1(n), \\ g_2(n), & \text{if } R_2(n), \\ g_3(n), & \text{if } R_3(n), \end{cases}$$

where

$$\begin{aligned} R_1(n) &\iff n = 2 \\ R_2(n) &\iff n = 3 \\ R_3(n) &\iff \text{not } R_1(n) \text{ and not } R_2(n) \end{aligned}$$

and

$$g_1(n) = 2, \quad g_2(n) = 3, \quad g_3(n) = 8.$$

It is easy to see that the relations R_1, R_2 and R_3 are mutually exclusive and exhaustive.

The characteristic function of R_1 is given by

$$\chi_{R_1}(n) = \chi_{eq}(n, 2),$$

which is primitive recursive as it is obtained by substitution from the primitive recursive function χ_{eq} using constants. Hence the relation R_1 is primitive recursive.

Similarly the characteristic function of R_2 given by

$$\chi_{R_2}(n) = \chi_{eq}(n, 3),$$

is primitive recursive. Hence the relation R_2 is primitive recursive.

That the relation R_3 is primitive recursive follows from Problem 1.10 of *Unit 2*.

Each of the functions g_1, g_2 and g_3 is a constant function and is thus primitive recursive.

Therefore, by Theorem 1.5 of *Unit 2*, the function f is primitive recursive, and hence total recursive, so that the set $\{2, 3, 8\}$ is recursive enumerable.

Solution 2.2

The empty set is recursively enumerable by definition. So we need only consider the case of a finite non-empty set, say $A = \{n_1, n_2, \ldots, n_k\}$. One suitable function f is given by

$$f(n) = \begin{cases} n_1, & \text{if } n = n_1, \\ n_2, & \text{if } n = n_2, \\ \vdots & \vdots \\ n_{k-1}, & \text{if } n = n_{k-1}, \\ n_k, & \text{otherwise.} \end{cases}$$

The function f can be shown to be primitive recursive, and hence total recursive, along similar lines to Solution 2.1 and clearly $A = \{f(0), f(1), f(2), \ldots\}$. Hence A is recursively enumerable.

Solution 2.3

Suppose A is a recursive set of natural numbers. If A is empty, then A is recursively enumerable by definition. So we can suppose that A is not empty. Let n_0 be the smallest number in A. The characteristic function χ_A of A is recursive and total. Now let f be the total function defined by

$$f(n) = \begin{cases} n, & \text{if } n \in A, \\ n_0, & \text{if } n \notin A. \end{cases}$$

Then

$$f(n) = n\chi_A(n) + n_0\,\overline{\mathrm{sg}}(\chi_A(n)),$$

so that f is obtained by substitution from the recursive functions χ_A, add, mult and $\overline{\mathrm{sg}}$ using constants. Thus f is a recursive function. Also $A = \{f(0), f(1), f(2), \ldots\}$. Hence A is recursively enumerable.

Solution 3.1

Let $\phi(x)$ be the formula $(\mathbf{0} \cdot x) = \mathbf{0}$. We shall follow the strategy of Example 3.2. Consider the following formal proof.

1	(1)	$\forall x\,(x + \mathbf{0}) = x$	Ass
2	(2)	$\forall x\,(x \cdot \mathbf{0}) = \mathbf{0}$	Ass
3	(3)	$\forall x\,\forall y\,(x \cdot y') = ((x \cdot y) + x)$	Ass
4	(4)	$\phi(x)$	Ass
2	(5)	$\phi(\mathbf{0})$	UE, 2
3	(6)	$\forall y\,(\mathbf{0} \cdot y') = ((\mathbf{0} \cdot y) + \mathbf{0})$	UE, 3
3	(7)	$(\mathbf{0} \cdot x') = ((\mathbf{0} \cdot x) + \mathbf{0})$	UE, 6
1	(8)	$((\mathbf{0} \cdot x) + \mathbf{0}) = (\mathbf{0} \cdot x)$	UE, 1
1, 3	(9)	$(\mathbf{0} \cdot x') = (\mathbf{0} \cdot x)$	Sub, 7, 8
1, 3, 4	(10)	$\phi(x')$	Sub, 4, 9
1, 3	(11)	$(\phi(x) \rightarrow \phi(x'))$	CP, 10
1, 3	(12)	$\forall x\,(\phi(x) \rightarrow \phi(x'))$	UI, 11
13	(13)	$((\phi(\mathbf{0})\ \&\ \forall x\,(\phi(x) \rightarrow \phi(x'))) \rightarrow \forall x\,\phi(x))$	Ass
1, 2, 3, 13	(14)	$\forall x\,\phi(x)$	Taut, 5, 12, 13

Assumptions 1, 2 and 3 are axioms $Q4$, $Q6$ and $Q7$, and assumption 13 is an induction axiom. It therefore follows that $\vdash_{\mathrm{PA}} \forall x\,\phi(x)$, that is $\vdash_{\mathrm{PA}} \forall x\,(\mathbf{0} \cdot x) = \mathbf{0}$.

Solution 3.2

Following the hint we show that

$$\vdash_Q (\forall x\,(\mathbf{0}+x) = x \rightarrow \forall x\,(x \cdot \mathbf{0}') = x) \tag{S.1}$$

Consider the following formal proof.

1	(1)	$\forall x\,(\mathbf{0}+x) = x$	Ass
2	(2)	$\forall x\,(x \cdot \mathbf{0}) = \mathbf{0}$	Ass
3	(3)	$\forall x \forall y\,(x \cdot y') = ((x \cdot y) + x)$	Ass
3	(4)	$\forall y\,(x \cdot y') = ((x \cdot y) + x)$	UE, 3
3	(5)	$(x \cdot \mathbf{0}') = ((x \cdot \mathbf{0}) + x)$	UE, 4
2	(6)	$(x \cdot \mathbf{0}) = \mathbf{0}$	UE, 2
2, 3	(7)	$(x \cdot \mathbf{0}') = (\mathbf{0} + x)$	Sub, 5, 6
1	(8)	$(\mathbf{0}+x) = x$	UE, 1
1, 2, 3	(9)	$(x \cdot \mathbf{0}') = x$	Sub, 7, 8
1, 2, 3	(10)	$\forall x\,(x \cdot \mathbf{0}') = x$	UI, 9
2, 3	(11)	$(\forall x\,(\mathbf{0}+x) = x \rightarrow \forall x\,(x \cdot \mathbf{0}') = x)$	CP, 10

Since assumptions 2 and 3 are axioms $Q6$ and $Q7$, this formal proof shows that (S.1) holds. In Example 3.2 we showed that

$$\vdash_{\mathrm{PA}} \forall x\,(\mathbf{0}+x) = x \tag{S.2}$$

Hence, applying the Tautology Rule to (S.1) and (S.2) shows that $\vdash_{\mathrm{PA}} \forall x\,(x \cdot \mathbf{0}') = x$.

Solution 3.3

Let $\phi(x)$ be the formula $\forall y \forall z\,((y+z)+x) = (y+(z+x))$.

We show first that $\vdash_Q \phi(\mathbf{0})$. Consider the following formal proof.

1	(1)	$\forall x\,(x+\mathbf{0}) = x$	Ass
1	(2)	$((y+z)+\mathbf{0}) = (y+z)$	UE, 1
1	(3)	$(z+\mathbf{0}) = z$	UE, 1
	(4)	$(z+\mathbf{0}) = (z+\mathbf{0})$	II
1	(5)	$z = (z+\mathbf{0})$	Sub, 3, 4
1	(6)	$((y+z)+\mathbf{0}) = (y+(z+\mathbf{0}))$	Sub, 2, 5
1	(7)	$\forall z\,((y+z)+\mathbf{0}) = (y+(z+\mathbf{0}))$	UI, 6
1	(8)	$\forall y \forall z\,((y+z)+\mathbf{0}) = (y+(z+\mathbf{0}))$	UI, 7

Since assumption 1 is axiom $Q4$, this shows that $\vdash_Q \phi(\mathbf{0})$.

Next we show that $\vdash_Q \forall x\,(\phi(x) \to \phi(x'))$. Consider the following formal proof.

1	(1)	$\forall x\,\forall y\,(x + y') = (x + y)'$	Ass
2	(2)	$\phi(x)$	Ass
2	(3)	$\forall z\,((y + z) + x) = (y + (z + x))$	UE, 2
2	(4)	$((y + z) + x) = (y + (z + x))$	UE, 3
1	(5)	$\forall y\,(w + y') = (w + y)'$	UE, 1
1	(6)	$(w + x') = (w + x)'$	UE, 5
1	(7)	$\forall w\,(w + x') = (w + x)'$	UI, 6
1	(8)	$((y + z) + x') = ((y + z) + x)'$	UE, 7
1, 2	(9)	$((y + z) + x') = (y + (z + x))'$	Sub, 4, 8
1	(10)	$\forall x\,\forall w\,(w + x') = (w + x)'$	UI, 7
1	(11)	$\forall w\,(w + (z + x)') = (w + (z + x))'$	UE, 10
1	(12)	$(y + (z + x)') = (y + (z + x))'$	UE, 11
	(13)	$(y + (z + x)') = (y + (z + x)')$	II
1	(14)	$(y + (z + x))' = (y + (z + x)')$	Sub, 12, 13
1, 2	(15)	$((y + z) + x') = (y + (z + x)')$	Sub, 9, 14
1	(16)	$(z + x') = (z + x)'$	UE, 7
	(17)	$(z + x') = (z + x')$	II
1	(18)	$(z + x)' = (z + x')$	Sub, 16, 17
1, 2	(19)	$((y + z) + x') = (y + (z + x'))$	Sub, 15, 18
1, 2	(20)	$\forall z\,((y + z) + x') = (y + (z + x'))$	UI, 19
1, 2	(21)	$\phi(x')$	UI, 20
1	(22)	$(\phi(x) \to \phi(x'))$	CP, 21
1	(23)	$\forall x\,(\phi(x) \to \phi(x'))$	UI, 22

Since assumption 1 is axiom $Q5$, it follows that $\vdash_Q \forall x\,(\phi(x) \to \phi(x'))$.

As the theory PA extends the theory Q, this means that

$$\vdash_{\mathrm{PA}} \phi(\mathbf{0}) \quad \text{and} \quad \vdash_{\mathrm{PA}} \forall x\,(\phi(x) \to \phi(x'))$$

Combining these proofs in PA with the induction axiom

$$((\phi(\mathbf{0})\ \&\ \forall x\,(\phi(x) \to \phi(x'))) \to \forall x\,\phi(x))$$

enables us to deduce that $\vdash_{\mathrm{PA}} \forall x\,\phi(x)$, that is

$$\vdash_{\mathrm{PA}} \forall x\,\forall y\,\forall z\,((y + z) + x) = (y + (z + x))$$

INDEX

GN(*T*) 7
PA 18
Prov(x) 23
$\delta(j)$ 13
$\phi(\mathbf{n})$ 17
$\phi(\tau)$ 17
$\Gamma(F)$ 13

axiomatizable
    recursively 11

Cantor 26
Church 27
Church's Theorem 10

enumerable
    recursively 11

Frege 27

Gödel 28
Gödel's First Incompleteness Theorem 15
Gödel's Second Incompleteness Theorem 25

Hilbert 28
Hilbert's Question 16, 22, 26

induction axioms 18

Kleene 28

Löb's Theorem 24
Leibniz 29
Leibniz's Question 4, 8

Mathematical Induction 17

Peano 29
Peano Arithmetic 18
Post 29
Principle of Mathematical Induction 17
provability predicate 23

recursive set of axioms 11
recursive set of theorems 11
recursively axiomatizable 11
recursively enumerable 11
representable set 5
Russell 30

Turing 30